Infoblox

The Infoblox Q4 2020

Cyberthreat Intelligence Report

Disclaimer

Infoblox publications and research are made available solely for general information purposes. The information contained in this publication is provided on an “as is” basis. Infoblox accepts no liability for the use of this data. Any additional developments or research since the date of publication will not be reflected in this report.

Table of Contents

Executive Summary

Infoblox is pleased to publish this edition of our Quarterly Cyberthreat Intelligence Report. We publish these reports during the first month of each calendar quarter. This Q4 2020 report includes our publicly released threat intelligence from October 1, 2020, through December 31, 2020.

This publication provides our original research and insight into threats we observed, detailed analysis of advanced malware campaigns and analysis of recent significant attacks. In some cases, we share and expand on original research published by other security firms, industry experts and university researchers. We feel that timely information on cyberthreats is vital to protect the user community at large.

Infoblox Cyberthreat Intelligence Reports generally include research on specific threats and related data, customer impacts, analysis of campaign execution and attack chains, as well as vulnerabilities and mitigation steps. We may also share background information on the attack groups likely responsible for the particular threats under review.

Subscribers to our threat intelligence products and services will receive the full reports, which provide more comprehensive data, including an in-depth list of the indicators of compromise (IOCs) for the specific campaign, as well as other timely alerts and information.

The 2021 Cyberthreats in Context

In the widespread transition to cloud computing, many organizations have transferred their legacy applications to infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) platforms. They have also expanded their use of software as a service (SaaS) to meet enterprise application requirements, resulting in a broad distribution of sensitive information across a variety of cloud platforms. Many organizations, however, still do not have a significant security for their cloud deployments. The existing enterprise security stack, including security controls such as data loss protection, cannot scale to the cloud.

New controls to secure container-based workloads, lock down cloud configurations and encrypt data in the cloud are still being deployed. Email, social media and collaborative software have created more vectors than ever for threat actors to target organizations. Infection from malware can result in the loss of sensitive data and open channels for threat actors to target more victims.

A study by the University of Maryland Clark School's Center for Risk and Reliability and Institute for Systems Research quantified the average rate of cyberattacks on computers with Internet access as occurring every 39 seconds. Every day, government institutions and private industries must manage cyberthreats from nation state–funded attackers or their proxies. Key enablers such as Bitcoin and other cybercurrencies make it much more challenging for law enforcement to identify and track threat actors.

The high number of employees teleworking during the pandemic has exacerbated the problem. Working remotely presents vulnerabilities that are more easily exploited by threat actors. Teleworkers require access to enterprise resources from multiple endpoints, including both employer-provided and personal laptops, as well as a variety of mobile devices.

However, many cybersecurity procedures and security controls used within enterprise facilities cannot provide the same level of security for remote locations. The on-premises legacy enterprise security stack will not work for remote workers without significant redesign, planning and a move to new security controls to support distributed infrastructure and cloud deployments. Domain Name System (DNS) security can be configured to protect teleworkers, but many organizations don't yet have the additional protections and visibility that DNS security deployment would provide. The same is true for expanded threat intelligence data: It can be tremendously useful, but only if you have it.

The situation is further complicated by teleworkers who must use personal “untrusted” devices to access critical corporate resources and information. This remote access must be granted not only to employees but also to business partners and contractors. They must access resources on-premises, behind the legacy firewall and in a multitude of SaaS, IaaS and PaaS clouds.

As of the end of 2020, many organizations have still not implemented necessary cybersecurity to protect this far more distributed user base. Email, a vital and essential tool, remains the top threat vector used to attack both government and businesses of all sizes. Despite training and warnings, users continue to open suspicious emails, both in their business and personal accounts. They click on malicious email attachments and URLs and view websites not generally associated with business use. Proprietary business information is at risk when workers use personal and business instances of applications such as Office 365 on the same machines, collaborate within clouds and connect to an ever-increasing number of SaaS clouds that are not work related and not sanctioned by their IT department.

For all of these reasons and more, cyberthreats remain alive and well. Threat actors will innovate, adjust and sustain proven methods in 2021. Rogue nation-states and organized crime will continue to build on their offensive capabilities. Accurate intelligence about timely, relevant threats enables an organization to make thoughtful, targeted improvements to its defenses and lower its risk.

Cybertrends

Email, Phishing and Social Engineering Remain Attackers' Threats of Choice

As in previous quarters, the Infoblox Cyber Intelligence Unit (CIU) observed extensive threat actor use of socially engineered email campaigns to propagate a variety of attacks. Phishing emails spoof communications that appear to come from a reputable source. The goal is often to steal sensitive information such as authentication data, install malware or obtain other financial resources such as credit card numbers. In some instances, these attacks are highly targeted to one individual or organization (spear-phishing), but larger campaigns are more common.

Socially engineered phishing emails persuade recipients to click on a link to a malicious site or file, or to open an attachment—often a compressed file or a Microsoft Office file. In many of the campaigns the CIU observed, recipients also had to enable editing or macros for the infection to commence.

Over the last three months, the CIU has published reports on campaigns delivering:

- Emotet banking trojan
- 404 Keylogger
- IcedID banking trojan
- Remcos remote access trojan (RAT)
- Adwind RAT
- AZORult infostealer
- Formbook infostealer
- Agent Tesla keylogger
- Abracadabra trojan
- LokiBot infostealer
- AveMaria RAT
- Hancitor trojan downloader

Consistent with our CIU's research, the European Union Agency for Cybersecurity (ENISA) published a report on phishing in October 2020 and noted that "attacks include schemes like business email compromise (BEC) and identity deception techniques based on social engineering to make phishing campaigns more effective." ENISA further noted that "over 99% of e-mails distributing malware required human intervention—following links, opening documents, accepting security warnings, and other behaviors—to be effective."

Cybersecurity Regulation

On December 4, 2020, the Internet of Things Cybersecurity Improvement Act of 2020 became law. This bill requires the National Institute of Standards and Technology (NIST) to develop standards and guidelines for the use of Internet of Things (IoT) devices owned or controlled by federal agencies. Ultimately any IoT devices acquired by the federal government must comply fully with these standards. Consumers will also be the beneficiaries as they purchase devices designed in compliance with the standard.

There are hundreds of bills or resolutions that deal with cybersecurity in the process of becoming law. This cybersecurity legislation is moving through state and local government in the United States and is likely to impact compliance and governance in many areas.

Q4 2020
Threat Report Summaries

Realistic Delivery Notices Drop Dridex Banking Trojan

On September 24, the CIU observed a malspam campaign distributing the Dridex banking trojan via emails spoofing FedEx package delivery notifications. In previously reported Dridex campaigns, the emails masqueraded as notifications from other legitimate companies, such as Automatic Data Processing, Inc. (ADP), eFax and Intuit.

404 Keylogger Campaigns

On October 11 and 15, the CIU observed two related malspam campaigns that used 7-Zip archive files to deliver the 404 Keylogger malware.

Emotet Gets Political

From October 16 to 19, the CIU observed a malspam campaign that referenced political themes in the subject lines of the emails and in the attached file name. The campaign distributed the Emotet banking trojan. The threat actors spreading Emotet have previously used popular topics such as COVID-19 as lures.

Formbook Infostealer Campaigns Continue

On October 30, the CIU observed a malicious email campaign distributing Formbook malware via Roshal Archive (RAR) attachments that contained a malicious binary executable file. Emails in this campaign leveraged a SWIFT invoice lure to persuade victims to open and run the attached files.

The CIU has observed and reported on several Formbook campaigns in the past. Some of these campaigns used SWIFT lures to entice victims into opening malicious file attachments, while others used lures like the ongoing COVID-19 pandemic.

AZORult Infostealer

From November 3 to 4, the CIU observed fashion- and beauty-themed malspam campaigns that delivered the AZORult infostealer via Microsoft Excel spreadsheets with malicious macros. These spreadsheets used living off the land (LotL) techniques that abused pre-existing software on the victim's machine to perform malicious tasks.

Remcos RAT Malspam Campaign

During the week of November 9, the CIU discovered a malspam campaign distributing the Remcos RAT. The emails in this campaign carried malicious Microsoft Office documents that required the user to enable macros to execute the Remcos payload. The CIU previously reported on a Remcos campaign in July 2019 that distributed Rich Text Format (RTF) files and exploited the Microsoft Equation Editor remote code execution vulnerability.

Automotive-Themed Malspam Delivers Adwind RAT

From November 12 to 13, the CIU observed a malicious email campaign distributing the Adwind remote access trojan (RAT) via a spoofed O'Meara Auto Group invoice using Microsoft Excel spreadsheets (XLS) with malicious macros.

Shathak Pushes IcedID in Japanese Malspam

On November 20, security researcher Brad Duncan reported on a malicious spam campaign from the threat actor known as Shathak (aka TA551) to distribute the IcedID banking trojan via emails written in Japanese. The CIU previously reported on a campaign in July wherein threat actors used a Valak downloader to deliver IcedID.

Hancitor Downloader and Follow-On Malware

Between November 23 and December 8, the CIU observed multiple malspam campaigns that all used DocuSign-themed lures to entice users to download and open Microsoft Word documents with malicious macros that install embedded copies of the Hancitor trojan downloader.

AveMaria RAT Malspam Campaign

Between December 2 and 7, the CIU observed a malicious email campaign distributing the AveMaria remote access trojan (RAT). In this campaign, threat actors used subjects referencing text message logs to lure users into opening a malicious Rich Text Format (RTF) file attachment that was disguised as a Microsoft Word document (DOC). The CIU previously reported on an AveMaria campaign in April 2019 that used shipping lures and contained similar malicious DOC files.

LokiBot Campaign Uses Microsoft Office Exploit

On December 9, the CIU observed a malicious email campaign exploiting CVE 2017-11882 to distribute LokiBot malware. This campaign used purchase order–themed lures to entice victims into downloading malicious Microsoft Excel files.

The CIU has previously written several reports on LokiBot, including on campaigns that used coronavirus-themed lures, NGROK tunneling to download payloads and malicious RTF files to infect victims. CVE 2017-11882, a stack buffer overflow vulnerability in the Microsoft Equation Editor, is an exploit commonly used by threat actors.

Encrypted Excel Files Drop Abracadabra Trojan

From December 13 to 14, the CIU observed a spam email campaign distributing a trojan known as Abracadabra via an encrypted Microsoft Excel spreadsheet with malicious macros. In this campaign, threat actors used an email subject referencing an overdue invoice to lure users into opening the malicious attachment.

Malspam Sender Spoofing Indian Companies Drops Agent Tesla Keylogger

Between December 13 and 14, the CIU observed a malspam campaign distributing Agent Tesla keylogger via a Microsoft Excel spreadsheet with malicious macros. In this campaign, threat actors sent emails spoofing communication from Gopaldas & Sons (also Gopal Das & Sons, both of which represent several large companies in India).

October 2020

Threat Reports &

Cyberthreat Alerts

Realistic Delivery Notices Drop Dridex Banking Trojan

Author: Eric Patterson

Overview

On September 24, Infoblox observed a malicious spam (malspam) email campaign distributing the Dridex banking trojan via emails spoofing FedEx package delivery notifications.[1]

In previously reported Dridex campaigns, the emails masqueraded as notifications from other legitimate companies such as Automatic Data Processing, Inc. (ADP), eFax, and Intuit.[2,3,4]

Customer Impact

Dridex was first discovered in 2011 and has consistently been one of the most prolific banking trojans on the market.[5] Threat actors typically favor this malware for large scale, financially-motivated malspam campaigns.

Once a victim is infected, Dridex uses its core functionalities of website injections and form grabbing to siphon online banking credentials and pilfer funds from the victims.

Campaign Analysis

Emails in this campaign imitate FedEx Shipment delivery notifications with subject lines containing *FedEx Shipment <fake 12-digit tracking number>: Delivered.* The message body itself uses HTML formatting to mimic the layout, format, and style of a standard FedEx delivery email. By all measurable standards, the malicious message body appears identical to legitimate emails sent by FedEx.

The email senders are slight variations of FedEx's legitimate email accounts.

The email infrastructure for delivering the Dridex malware includes fraudulent sites with a wide range of top-level domains (TLDs). The registration information for the associated domains also makes use of various registrars and nameservers with no discernable pattern or preference.

Attack Chain

Within the body of the message is a fake 12-digit tracking number that when clicked, automatically downloads a ZIP file to the victim's machine from one of many malicious hosting domains. Extracting the ZIP archive yields a screensaver file (SCR) with the same name as an Adobe PDF icon. This method of using SCR files with PDF icons is a well-known technique of Dridex and the banking malware community as a whole.

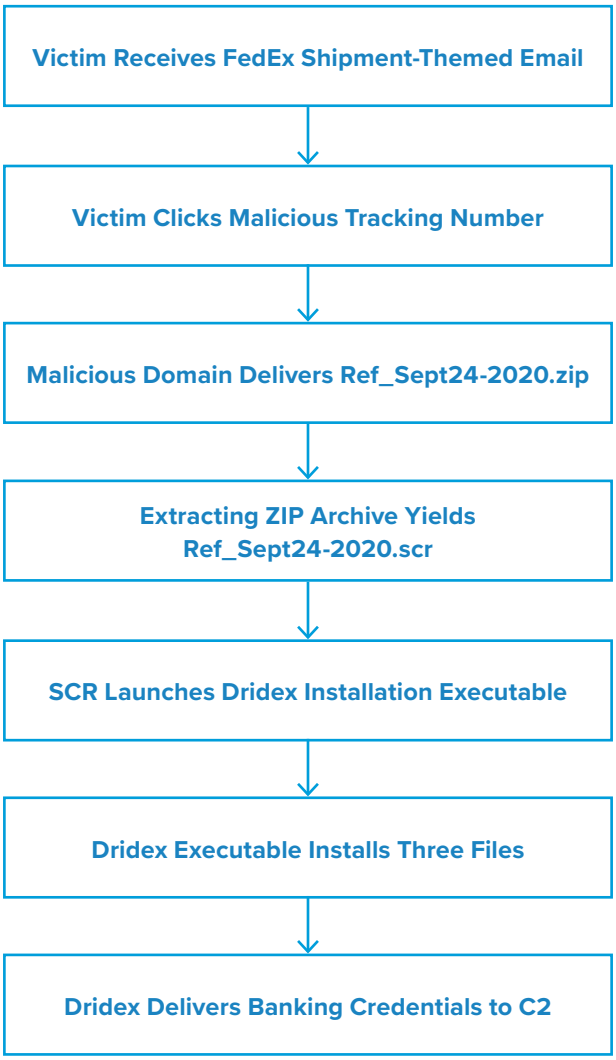
Clicking on the SCR file will launch the Dridex installation executable (EXE) of the same name, which then installs three dynamic-link library (DLL) files onto the victim's machine: *ACTIVEDS.dll*, *VERSION.dll*, and *DUI70.dll*. Each of these files is installed by a legitimate Windows process: *ApplySettingsTemplateCatalog.exe, ie4uinit.exe,* and *DmNotificationBroker.exe,* respectively.

Once installed, Dridex will attempt to uncover and steal sensitive banking information belonging to the victim and transmit that to one of its active command and control (C2) channels via SSL.[6]

Vulnerabilities & Mitigation

Dridex is a banking trojan that is equipped with credential stealing functions. Infoblox recommends the following methods for detecting, preventing, and mitigating Dridex attacks:

- Install and run advanced antivirus software that can detect, quarantine, and remove malware.
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Develop traffic rules that can block outbound access to potentially malicious endpoints based on domains or unique URI parameters.
- Implement PowerShell logging to detect any anomalous or malicious use.
- Install strong email security solutions to detect emails with suspicious content.



Endnotes

1. https://www.malware-traffic-analysis.net/2020/09/24/index.html
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--51
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--19
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--72
5. https://www.globenewswire.com/news-release/2020/04/09/2014156/0/en/March-2020-s-Most-Wanted-Malware-Dridex-Banking-Trojan-Ranks-On-Top-Malware-List-For-First-Time.html
6. https://www.joesandbox.com/search?q=fad001d463e892e7844040cabdcfa8f8431c07e7ef1ffd76ffbd190f49d7693d

404 Keylogger Campaigns

Author: James Barnett

Overview

On October 11 and 15, Infoblox observed two related malicious spam (malspam) campaigns that used 7-Zip archive files to deliver the 404 Keylogger malware.

Customer Impact

404 Keylogger is an information stealer (infostealer) that can steal a victim's credentials and log their keyboard input. It was initially released on a Russian hacking forum in August 2019.[1] It is notable for its relatively unusual methods of data exfiltration, including via email messages, Pastebin file uploads and encrypted Telegram messages.

Campaign Analysis

All malspam emails in the two campaigns we observed came from the same SMTP server, but each campaign had different themes for the subject lines and attachments. The October 11 campaign used the subject line *RE: BANK TRANSFER SLIP* and had an attachment named *swift transfer copy 639082020.7z*. The October 15 campaign used the subject line *Re: T21 Orders - Quotation - MLM -309-Ref-284* and included an attachment named *T21 Orders - Quotation 309-Ref-284.7z*.

Attack Chain

When the victim extracts and executes the 404 Keylogger payload contained within the 7-Zip archive, the malware creates a copy of itself with a randomized name in the victim's *AppData* folder. It then creates a scheduled task that will periodically run this copy of the malware, allowing it to achieve a basic level of persistence on the victim's machine.

After establishing persistence, 404 Keylogger sets up a keyboard hook that allows it to log the victim's keystrokes so that the attacker can steal any credentials the victim types in. The malware then proceeds to search for saved credentials for a variety of different application types, including web browsers (e.g. Google Chrome), email clients (e.g. Microsoft Outlook), chat clients (e.g. Pidgin) and FTP clients (e.g. Filezilla).

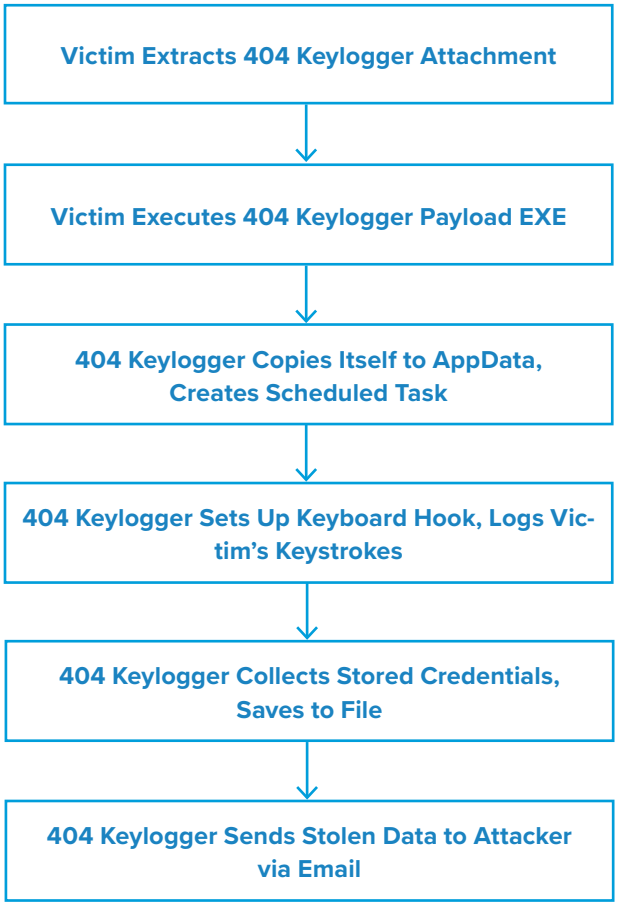
Once 404 Keylogger has collected the victim's credentials, it contacts a legitimate IP lookup service to determine the IP address of the victim's machine. It also gathers various pieces of information about the system itself, including the system name and Windows version. It then combines all of this information along with the stolen credentials and saves it in the current user's *Documents* folder as a text file named *Results.txt*.

When 404 Keylogger has saved all of the stolen information to a file, it uses one of its available data exfiltration methods to transfer the information to the attacker. While 404 Keylogger is known to be capable of exfiltrating data via Pastebin and Telegram, the campaigns we observed only used email messages for its data exfiltration.

Vulnerabilities & Mitigation

Infoblox recommends the following actions to reduce the risk of a 404 Keylogger infection:

- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.
- Do not allow web browsers such as Mozilla Firefox or Google Chrome to save credentials or other sensitive information.



Endnotes

1. https://www.lastline.com/labsblog/infostealers-weaponizing-covid-19/

change image

Cyberthreat Advisory: APT Groups Target U.S. Election

Author: Jeremy Ware & Darby Wise

Executive Summary

On December 15, Infoblox released a Cyber Threat Advisory On 22 October, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) published two joint advisories on Russian-state sponsored and Iranian advanced persistent threat actors (APTs) targeting various U.S. government networks and the upcoming U.S. election.[1,2]

In an ongoing campaign since September, a Russian state-sponsored APT, known by many names, including Berserk Bear, Energetic Bear, TeamSpy, Dragonfly, Havex, Crouching Yeti and Koala, has been targeting various aviation and U.S. state, local, territorial, and tribal (SLTT) government networks to steal credentials and ultimately exfiltrate any valuable data.

Iranian APTs known for a significant number of intrusions against various U.S. networks are now likely seeking to influence the upcoming election by spoofing media sites to spread anti-American propaganda and misinformation on voter suppression and fraud.

Analysis

Russian APTs

Since February, the Russian state-sponsored APT has been conducting brute force attacks and structured query language (SQL) injections, hosting malicious domains, as well as exploiting several Common Vulnerabilities and Exposures (CVEs) such as a Citrix Directory Traversal Bug (CVE-2019-19781)[3] and a Microsoft Exchange remote code execution flaw (CVE-2020-0688).[4] This APT is also known to utilize Cisco AnyConnect Secure Socket Layer (SSL) virtual private network (VPN) connections to enable remote logins on at least one victim's network, potentially by utilizing an Exim Simple Mail Transfer Protocol (SMTP) vulnerability (CVE 2019-10149)[5] (External Remote Services [T1133]).[6]

According to the report, most recent attacks by this APT exploited a Fortinet VPN vulnerability for Initial Access [TA0001],[7] along with the Windows Netlogon vulnerability (CVE-2020-1472).[8] The actor then pivoted to obtain access to Windows Active Directory (AD) servers to elevate their privileges [TA0004][9] within the network. The use of these vulnerabilities allows for the threat actors to compromise additional devices on the network and maintain persistence [TA0003].[10]

The APT used these techniques to target aviation and SLTT government networks, and has successfully exfiltrated data from at least two victim servers. This data includes sensitive network configurations, passwords, vendor and purchasing information, printing access badges and standard operating procedures (SOP). There is currently no direct evidence indicating this actor has already intentionally interfered with government, aviation, or U.S. election operations. However, the report suggests that this actor could be targeting the organizations to gain access for future operations targeting U.S. policies or SLTT government entities.to bypass the Duo multi-factor authentication (MFA) service and access a user's email via the Outlook Web App (OWA). While we are still investigating our non-Orion products, to date, we have not seen evidence that they are impacted by SUNBURST.

Iranian APTs

Since August 2019, Iranian APTs have carried out numerous attacks targeting U.S.-based networks. In these attacks, the actors have exploited several CVEs concerning content management systems (CMSs) and VPNs, including CVE-2020-5902[11] and CVE-2017-9248.[12] CVE-2020-5902 specifically highlights vulnerabilities in F5's BIG-IP VPNs that allow threat actors to execute arbitrary commands, disable services, etc.[13] CVE-2017-9248 references a weakness that exists in the Telerik UI dynamic-link library (DLL) *Telerik.Web.UI.dll*. This vulnerability could potentially result in cross-site scripting (XSS) attacks.[14]

According to the report, these actors have also conducted various kinds of attacks, including SQL injections and distributed denial-of-service (DDoS) attacks, website defacements, as well as spear-phishing and disinformation campaigns. The APTs have been combining these activities with the exploitation of certain CVEs to attempt to disrupt the upcoming U.S. presidential election.

- Threat actors use SQL injections to insert and execute malicious code in applications and websites. Injecting into the CMS of a media company or election-related website would give the actor access to the website's network, allowing them to manipulate its content and insert falsified information.
- The APT could use DDoS attacks to prevent users from accessing important online resources related to elections, such as websites with voting information or unofficial results. These attacks could flood election-related websites with server requests, potentially slowing them down to the point of being inaccessible.
- Similar to the SQL injections, threat actors can use website defacements to manipulate the content of an election-related website by compromising vulnerabilities in its CMS. Threat actors could delegitimize these websites and impact the public's view by uploading any kind of images to the website's landing page.
- Malspam campaigns use spear-phishing emails with malicious links or attachments to lure users into entering sensitive information such as credentials. Threat actors are then able to steal this information and use it to gain access to a victim's system. In this case, Iranian APTs could use the stolen credentials to access a victim's email and contact list to spread falsified information.
- Threat actors use disinformation campaigns to undermine confidence in the electoral system. These campaigns use social media, along with fake and spoofed media websites to spread falsified information to a large audience. Various social media companies have attempted to minimize these campaigns by removing posts with falsified news stories, along with the accounts that spread them, but these efforts are not enough to fully prevent this kind of malicious activity.

Prevention and Mitigation

ISA and the FBI provide a set of recommendations in each report to mitigate the effects of the APTs, including the following table with patch information on specific vulnerabilities targeted by the Russian APT:

Table 1. Patch information for CVEs[15]

Vulnerability	Vulnerable Products	Patch Information
CVE-2019-19781	Citrix Application Delivery Controller Citrix Gateway Citrix SDWAN WANOP	Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 11.1 and 12.0 Citrix blog post: security updates for Citrix SD-WAN WANOP release 10.2.6 and 11.0.3 Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway versions 12.1 and 13.0 Citrix blog post: firmware updates for Citrix ADC and Citrix Gateway version 10.5

Vulnerability	Vulnerable Products	Patch Information
CVE-2020-0688	Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 30 Microsoft Exchange Server 2013 Cumulative Update 23 Microsoft Exchange Server 2016 Cumulative Update 14	Microsoft Security Advisory for CVE-2020-0688
CVE-2020-0688	Microsoft Exchange Server 2016 Cumulative Update 15 Microsoft Exchange Server 2019 Cumulative Update 3 Microsoft Exchange Server 2019 Cumulative Update 4	Microsoft Security Advisory for CVE-2020-0688
CVE-2019-10149	Exim versions 4.87–4.91	Exim page for CVE-2019-10149
CVE-2018-13379	FortiOS 6.0: 6.0.0 to 6.0.4 FortiOS 5.6: 5.6.3 to 5.6.7 FortiOS 5.4: 5.4.6 to 5.4.12	Fortinet Security Advisory: FG-IR-18-384
CVE-2020-1472	Windows Server 2008 R2 for x64-based Systems Service Pack 1 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) Windows Server 2012 Windows Server 2012 (Server Core installation) Windows Server 2012 R2 Windows Server 2016 Windows Server 2019 Windows Server 2019 (Server Core installation)	Microsoft Security Advisory for CVE-2020-1472

	Windows Server, version 1903 (Server Core installation) Windows Server, version 1909 (Server Core installation) Windows Server, version 2004 (Server Core installation)	

Endnotes

1. https://us-cert.cisa.gov/ncas/alerts/aa20-296a
2. https://us-cert.cisa.gov/ncas/alerts/aa20-296b
3. https://nvd.nist.gov/vuln/detail/CVE-2019-19781
4. https://nvd.nist.gov/vuln/detail/CVE-2020-0688
5. https://nvd.nist.gov/vuln/detail/CVE-2019-10149
6. https://attack.mitre.org/versions/v7/techniques/T1133/
7. https://attack.mitre.org/versions/v7/tactics/TA0001/
8. https://nvd.nist.gov/vuln/detail/CVE-2018-13379
9. https://attack.mitre.org/versions/v7/tactics/TA0004/
10. https://attack.mitre.org/versions/v7/tactics/TA0003/
11. https://nvd.nist.gov/vuln/detail/CVE-2020-5902
12. https://nvd.nist.gov/vuln/detail/CVE-2017-9248
13. https://support.f5.com/csp/article/K52145254
14. https://www.telerik.com/support/kb/aspnet-ajax/details/cryptographic-weakness
15. https://us-cert.cisa.gov/ncas/alerts/aa20-296a

Emotet Gets Political

Author: Nick Sundvall

Overview

From October 16 to 19, we observed a malspam campaign that referenced political themes in the subject lines of the emails and in the attached file name. The campaign distributed the Emotet banking trojan. The threat actors spreading Emotet have previously used popular topics such as COVID-19 as lures.[1]

Customer Impact

Emotet is a notorious banking trojan and infostealer that was first observed in 2014.[2] Emotet can steal banking data and passwords from a victim's computer, as well as download and install additional malware such as Trickbot or Qakbot.[3] Once it downloads additional malware, it can then spread laterally across a network by sending malicious emails to contacts of the infected victim, carrying out brute force attacks and using Trickbot to launch exploits such as EternalBlue.[4]

Campaign Analysis

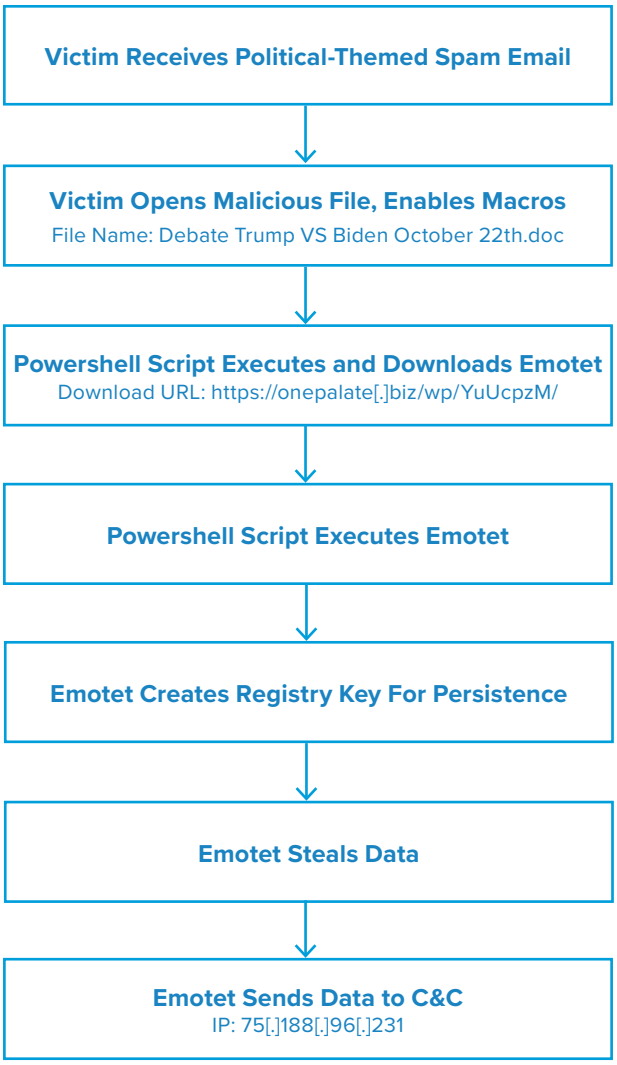
In this campaign, the threat actor used the upcoming presidential election as a lure by sending politically themed emails. Subjects of the emails included *Re: Trump-Ends Another Obama-Era Program and Marc*, *Save up to 30% on health insurance w/ TrumpCare*. Each of the emails had an attached file named *Debate Trump VS Biden October 22th.doc*, referencing the upcoming final presidential debate.

Attack Chain

Upon opening the attached file, the victim will see a document prompting them to upgrade Microsoft Word by clicking "Enable Editing and then click Enable Content." Following these instructions enables macros and allows the malicious Visual Basic for Applications (VBA) code to run.

Once the victim enables the macros, the VBA code executes a Powershell script containing several URLs. It attempts to reach out to each until it successfully downloads the malicious Emotet payload.

After downloading the payload, the script uses Windows Management Instrumentation (WMI) to execute the payload as *Yzsk_77.exe*. To maintain persistence, the executable then copies itself to a folder in the *%AppData%* directory, as well as creates a new registry key to run the Emotet executable anytime the user logs onto their computer. From here, Emotet connects to its command and control (C&C) server at *75[.]188[.]96[.]231* and sends the stolen data.



Vulnerabilities & Mitigation

Malspam email campaigns are a common distribution method for Emotet. Infoblox therefore recommends the following precautions to reduce the possibility of infection:

- Never configure Microsoft Office to enable macros by default. Many malware families use macros as an infection vector.
- Do not enable macros in Microsoft Office attachments, especially if the file's only apparent contents are directions to enable macros.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.
- Do not open attachments that are unexpected or from unfamiliar senders.

Appendix

Representative Indicators of Compromise	Description
Marc, Save up to 30% on health insurance w/ TrumpCare See Your 2019 TrumpCare Eligibility Review, Marc. Re: Trump-Ends Another Obama-Era Program	Email subject
Debate Trump VS Biden October 22th.doc	File attachment name
3bae78182dad47ac43920171f44e275863e25a8cbdd07ac0b0279edb751dd12a d684ed61705b1b1454f593263d3af902f854f6f32c217838fab990f4ad9d1a46 cfb29199ec6bb6dd95821e0506b52df13f7ac0f2a4579534454d7d6b025cdbc5 4f1b55b5cbbaa28b0d87b93dd256cebd16df18a51e081378940ad152fd24da8e	File attachment SHA256
https://onepalate[.]biz/wp/YuUcpzM/ https://webdachieu[.]com/wp-admin/J/ http://smallbatchliving[.]com/wp-admin/uccE/ http://richellemarie[.]com/wp-admin/xlTWW/ http://richelleshadoan[.]com/wp-admin/Ucrkcvp/ http://holonchile[.]cl/purelove/Y4/ http://a2zarchitect[.]com/wp-admin/LAs0P/ https://raumfuerneues[.]eu/error/AuTiH/	Download URLs
75[.]188[.]96[.]231	C&C server

Endnotes

1. https://securityintelligence.com/posts/emotet-activity-rises-as-it-uses-coronavirus-scare-to-infect-targets-in-japan/
2. https://www.malwarebytes.com/emotet/
3. https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service
4. https://securityboulevard.com/2019/10/a-closer-look-at-the-emotet-banking-trojan/

Cyberthreat Advisory: Kimsuki APT Update

Author: Nathan Toporek

Executive Summary

On October 27, 2020 the Cybersecurity Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the US Cyber Command Cyber National Mission Force (CNMF) published a joint report summarizing multiple OSINT publications that identifies several tactics, techniques, and procedures (TTPs) associated with the North Korean advanced persistent threat group (APT) Kimsuki.[1] Kimsuki used these TTPs to gather intelligence on behalf of the North Korean government.

The US Government refers to all malicious cyber activity from the North Korean Government as “HIDDEN COBRA.”

Analysis

The joint report found that Kimsuki has likely been active since 2012, and is likely tasked by the North Korean government with gathering intelligence on a global scale. Kimsuki uses social engineering tactics like spearphishing and watering hole attacks against victims; however, they are most likely to use spearphishing to gain initial access. Their past operations targeted experts, think tanks, and South Korean government groups using lures about foreign political issues, nuclear policy, and sanctions. The report details multiple Kimsuki TTPs, from initial access to exfiltration, each summarized below.

Initial Access (TA0001)

Kimsuki commonly uses spearphishing campaigns to gain initial access. The themes for campaigns often have to do with setting up a Skype interview with the victim where they appear on a television show. The first several emails may not contain malicious attachments, in an effort to build trust. At some point Kimsuki will deliver a malicious payload, and then cancel the interview. Other lures have included topics related to current events or issues of popular interest.

Execution (TA0002)

Kimsuki uses the Visual Basic malware family Babyshark to perform command execution via Windows PowerShell.[2]

Persistence (TA0003)

Kimsuki achieves persistence via malicious browser extensions, augmenting system processes, leveraging the autostart program, using the remote desktop protocol (RDP), and changing files associated with various applications.

Privilege Escalation (TA0004)

Kimsuki performs privilege escalation by editing startup programs, changing file associations, and process injection. They have also used Metasploit's "Win7Elevate" exploit to escalate privileges.

Defense Evasion (TA0005)

Kimsuki evades defenses by disabling the Windows firewall and disabling Windows security center service, deleting data after exfiltrating it to remove evidence, using trusted tools like mshta.exe to execute malicious JavaScript or Visual Basic script (VBS) files, and leveraging Metasploit's "Win7Elevate" exploit yet again to inject code into the Internet Explorer process.

Credential Access (TA0006)

Kimsuki accesses victim credentials with malicious Chrome browser extensions, Windows' *ProcDump* tool, a PowerShell-based keylogger named *MECHANICAL*, and specially-tailored versions of *PHProxy* (an open-source, PHP-based web proxy).

Discovery (TA0007)

Kimsuki appears to rely on native operating system commands to gather system information, which they likely exfiltrate to a command and control (C&C) server.

Collection (TA0009)

Kimsuki collects victim information via a malicious Hangul Word Processor (HWP) executable, keyloggers, and a Mac OS-specific Python tool designed to infect Mac OS systems. The HWP malware will email the contents of HWP files to actors prior to opening them for the user via a legitimate word processor.

Command and Control (TA0011)

Kimsuki performs C&C via a modified TeamViewer client that disables the firewall and configures several Windows registry keys that affect how the client connects to the server. At another time, Kimsuki will execute this malicious client.

Exfiltration (TA0010)

Kimsuki exfiltrates data by encrypting data and emailing it to C&C servers.

Prevention and Mitigation

CISA, the FBI, and CNMF recommend that users and organizations in Kimsuki's target profile implement protections against spearphishing, enable multi-factor authentication, and train users on phishing awareness.

Indicators of Compromise

The joint report provided multiple domains, and URL paths associated with the Kimsuki APT group.

Endnotes

1. "Joint Cybersecurity Advisory – US-Cert – CISA." 27 Oct. 2020, https://us-cert.cisa.gov/sites/default/files/publications/TLP-WHITE_AA20-301A_North_Korean_APT_Focus_Kimsuky.pdf. Accessed 28 Oct. 2020.
2. "BabyShark, Software S0414 | MITRE ATT&CK®." 7 Oct. 2019, https://attack.mitre.org/software/S0414/. Accessed 29 Oct. 2020.

November 2020

Threat Reports &

Cyberthreat Alerts

Cyberthreat Advisory: Iranian APT Exploits Election Websites

Author: Christopher Kim

Executive Summary

On October 30, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) published a joint advisory on Iranian advanced persistent threat actors (APTs) responsible for targeting U.S. state election websites and spreading disinformation about the 2020 U.S. presidential election via email.[1]

From September 20 to 28, the APT used a tool named Acunetix to scan state election websites for known web vulnerabilities. The actors used these vulnerabilities to exploit websites and steal voter registration data between September 29 and October 17. CISA and the FBI confirm that the actors successfully obtained voter registration data in at least one state.

Analysis

Reconnaissance

According to the advisory, the Iranian APT searched state voter websites for publicly available PDF documents by querying URLs with the words: *vote, voter, or registration*. The FBI also found information indicating that the actors researched the following topics to extend their capabilities for vulnerability identification and exploitation:

- YOURLS exploit
- Bypassing ModSecurity Web Application Firewall
- Detecting Web Application Firewalls
- SQLmap tool

Web Vulnerability Scanning

Between September 20 and 28, the APT actors attempted SQL injections across multiple state election websites by using the web vulnerability scanner Acunetix. This is a legitimate scanner often used by security engineers for security and compliance auditing. The actors used this tool to insert data into various fields in the /registration/ registration/details resource path on the web server. CISA analysts discovered 3 different web browser user agents associated with the scanning and observed the following requests:

2020-09-26 13:12:56 x.x.x.x GET /x/x v[$acunetix]=1 443 – x.x.x.x Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 – 200 0 0 0

2020-09-26 13:13:19 X.X.x.x GET /x/x voterid[$acunetix]=1 443 – x.x.x.x Mozilla/5.0+(Windows+NT+6.1;+WOW64)+AppleWebKit/537.21+(KHTML,+like+Gecko)+Chrome/41.0.2228.0+Safari/537.21 – 200 0 0 1375

2020-09-26 13:13:18 .X.x.x GET /x/x voterid=;print(md5(acunetix_wvs_security_test)); 443 – X.X.x.x

Data Exfiltration

Between September 29 and October 17, the APT sent several hundred thousand HTTP GET queries to web resources that hold voter registration data. The threat actor used the cURL command-line tool and free download manager (FDM) user agents to send the requests, as well as modified the request parameters by iterating through voter identification values as shown below.

2020-10-17 13:07:51 x.x.x.x GET /x/x voterid=XXXX1 443 – x.x.x.x curl/7.55.1 – 200 0 0 1406

2020-10-17 13:07:55 x.x.x.x GET /x/x voterid=XXXX2 443 – x.x.x.x curl/7.55.1 – 200 0 0 1390

2020-10-17 13:07:58 x.x.x.x GET /x/x voterid=XXXX3 443 – x.x.x.x curl/7.55.1 – 200 0 0 1625

2020-10-17 13:08:00 x.x.x.x GET /x/x voterid=XXXX4 443 – x.x.x.x curl/7.55.1 – 200 0 0 1390

Prevention and Mitigation

CISA and the FBI recommend the following actions for detecting, preventing and mitigating similar malicious activities described in this report.

Detecting Acunetix

Organizations that rarely use the Acunetix tool should monitor logs for any indication of the program's activity. The following keywords can help organizations identify Acunetix during log analysis:

- $acunetix
- acunetix_wvs_security_test

Other Recommendations

- Validate input as a method of sanitizing untrusted input submitted by web application users. Validating input can significantly reduce the probability of successful exploitation by protecting against security flaws in web applications. The types of attacks this could help prevent include SQL injection, cross site scripting (XSS), and command injection.
- Audit the organization's network for systems using Remote Desktop Protocol (RDP) and other internet-facing services. Disable unnecessary services and install available patches for the services in use. Users may need to work with their technology vendors to confirm that patches will not affect system processes.
- Verify all cloud-based virtual machine instances with a public IP, and avoid using open RDP ports, unless there is a valid need. Place any system with an open RDP port behind a firewall and require users to use a VPN to access it through the firewall.
- Enable strong password requirements and account lockout policies to defend against brute-force attacks.
- Apply multi-factor authentication when possible.
- Maintain a good information back-up strategy by routinely backing up all critical data and system configuration information on a separate device. Store the backups offline, verify their integrity, and verify the restoration process.
- Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- Ensure third parties that require RDP access follow internal remote access policies.
- Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.
- Regulate and limit external to internal RDP connections. When external access to internal resources is required, use secure methods, such as a VPN. However, recognize the security of the VPNs match the security of the connected devices.
- Use security features provided by social media platforms; use strong passwords, change passwords frequently, and use a different password for each social media account.
- See CISA's Tip on Best Practices for Securing Election Systems for more information.

Endnotes

1. https://us-cert.cisa.gov/ncas/alerts/aa20-304a

change image

Cyberthreat Advisory: Ransomware Attacks Target Healthcare Sector

Author: Jeremy Ware and Darby Wise

Executive Summary

On October 28, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Health and Human Services (HHS) published a joint advisory on threat actors targeting the Healthcare and Public Health (HPH) sector.[1] This report details the threat actors' use of Trickbot and BazarLoader malware to distribute ransomware, steal sensitive data, and attempt to interfere with healthcare services.

BazarLoader and Trickbot are two malware loaders that threat actors tend to distribute via phishing campaigns. In these attacks targeting U.S. hospitals and healthcare providers, threat actors used these loaders to distribute follow-on malware including Ryuk and Conti ransomware.

The report also details a new malware tool from the Trickbot developers called anchor_dns. This tool is a part of Anchor, a Trickbot module first observed in 2019, when it was used against large corporations and other high-profile organizations. Threat actors use anchor_dns to send and receive sensitive data from the victim's machine via Domain Name System (DNS) tunneling.

The joint report included a list of indicators of compromise (IOCs) associated with Trickbot, anchor_dns and BazarLoader, many of which Infoblox has incorporated into its security products since April of this year. We included the full list of indicators at the end of this report, along with additional IOCs we were able to find in our own research.

Analysis

Trickbot and Anchor_dns

Trickbot is a banking trojan that was first discovered in 2016. Threat actors primarily distribute it through malspam campaigns, or as a secondary payload to other malware such as Emotet. Since its initial discovery, Trickbot has evolved to include a full suite of tools to harvest credentials, deploy cryptominers or ransomware, and exfiltrate a multitude of data types. For a detailed analysis of Trickbot's attack chain, see the joint advisory or one of Infoblox's previous reports on this malware.[2,3]

Anchor_dns is a backdoor tool created by the Trickbot developers as part of the toolset module named Anchor.[4] With anchor_dns, threat actors communicate between the victim's machine and the command and control (C&C) servers via DNS tunneling to mimic legitimate traffic and thereby evade detection. Anchor_dns is also known to use an 'exclusive or' (XOR) cipher for encryption with the key *0xB9*.

BazarLoader and BazarBackdoor

BazarLoader and BazarBackdoor are believed to have been created by the threat actors behind Trickbot and were first observed in early 2020. They work together to infect the victim's machine, communicate with the C&Cs, and according to the alert have become increasingly popular means of deploying ransomware. In the attack against the HPH sector, they downloaded Ryuk and Conti ransomware.

Threat actors have distributed BazarLoader two ways: first, via phishing emails that carry malicious attachments; second, via links directing users to malicious DOC or PDF file on a legitimate document hosting site such as Google Drive.[5] Once the user downloads the file, BazarLoader drops the payload for BazarBackdoor, which the threat actor then uses to exploit the host machine and network.

Ryuk Ransomware

Threat actors often distribute Ryuk ransomware as a follow-on payload from banking trojans such as Trickbot or Emotet. Ryuk is a derivative of Hermes,[6] a ransomware variant that injects malicious dynamic-link library (DLL) files into the memory of the victim's machine, and then spreads laterally across a victim's network. Once the Ryuk payload is dropped, it uses Advanced Encryption Standard (AES)-256 keys to encrypt the victim's files. The ransomware then drops a RyukReadMe file on the victim's machine instructing them to contact a provided Protonmail-encrypted email address for further instructions on the ransom amount and specific Bitcoin wallet to which the victim must submit their payment. Infoblox has previously written on Ryuk, providing an in-depth analysis on its distribution, attack chain, etc. For a more detailed attack chain, refer to the joint advisory or our previous report on Ryuk.[7]

Prevention and Mitigation

CISA, FBI and HHS provide a set of recommendations to prevent or mitigate the effects of these kinds of cyberattacks. We include some below but a more extensive list, including preventative measures against specific ransomware, can be found in the joint report.

Network best practices:

- Patch operating systems, software, and firmware as soon as manufacturers release updates.
- Regularly validate secure configurations and ensure local administration is enabled for all operating systems of organization-owned assets.
- Regularly change passwords to network systems and accounts and avoid reusing passwords for different accounts.
- Use multi-factor authentication where possible.
- Disable unused remote access/Remote Desktop Protocol (RDP) ports and monitor remote access/RDP logs.
- Implement application and remote access allow listing to only allow systems to execute programs known and permitted by the established security policy.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Audit logs to ensure new accounts are legitimate.
- Scan for open or listening ports and mediate those that are not needed.
- Identify critical assets; create backups of these systems and house the backups offline from the network.
- Implement network segmentation. Sensitive data should not reside on the same server and network segment as the email environment.
- Set antivirus and anti-malware solutions to automatically update; conduct regular scans.

Ransomware mitigation best practices:

- Regularly back up data, air gap, and password protect backup copies offline.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, secure location.

Endnotes

1. https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--77
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence–66
4. https://cyware.com/news/trickbot-anchor-malware-infects-both-linux-and-windows-systems-cfbe68d7
5. https://isc.sans.edu/forums/diary/ BazarLoader+phishing+lures+plan+a+Halloween+party+get+a+bonus+and+be+fired+in+the+same+afternoon/26710/?_hsmi=98108296&_hsenc=p2ANqtz–ljGhOfCvkpHP8QWsJI_dK73jhzUQ9j6RbjdLkFIt6nKwC8do9_OP1H0Q48uebHH3uwRmjJrDysxbqidQpjcy1LIVdm4yqXjEO27OANzPnnM6BoEE
6. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence–5
7. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence–3

Formbook Infostealer Campaigns Continue

Author: Nathan Toporek

Overview

On October 30, Infoblox observed a malicious email campaign distributing Formbook malware via Roshal Archive (RAR) attachments that contained a malicious binary executable file. Emails in this campaign leveraged a SWIFT invoice lure to persuade victims to open and run the attached files.

Infoblox has observed and reported on several Formbook campaigns in the past.[1,2,3,4,5] Some of these campaigns used SWIFT lures to entice victims into opening malicious file attachments, while others used lures like the ongoing COVID-19 pandemic. Threat actors commonly use financial lures and other "urgent" topics such as invoices to convince victims to open files.

Customer Impact

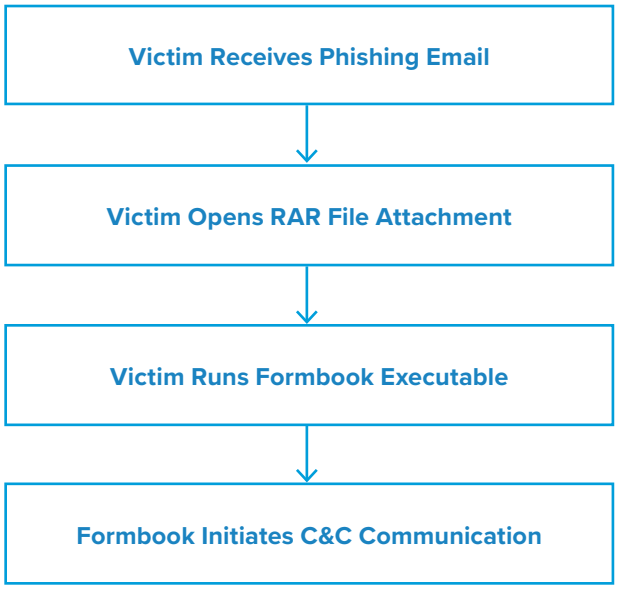
Formbook is an infostealer that is sold as a service to threat actors. Its capabilities include process hollowing, clipboard monitoring, keylogging, webform hijacking, screenshotting, downloading additional payloads and communicating with a command and control (C&C) server.

Campaign Analysis

In this campaign, victims received an email urging them to open the attached SWIFT invoice with the subject line *Re: Bank Swift TT copy*. The file attachment was a RAR file that contained a malicious executable file named *Swift TT Copy.exe*

Attack Chain

When the victim opens and runs the executable, it will infect their computer with Formbook. Formbook then injects itself into the Internet Explorer application and initiates communication with its C&C servers.



Vulnerabilities & Mitigation

This campaign relies on social engineering tactics to infect users with Formbook. As such, Infoblox recommends taking the following actions to reduce the likelihood of infection:

- Keep computers and all endpoints up to date with the latest security patches to block known vulnerabilities that threat actors could target.
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.

Endnotes

1. Infoblox Cyber Intelligence Unit. "Cyber Campaign Brief: Formbook Coronavirus Campaigns" April 2020. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--67
2. Infoblox Cyber Intelligence Unit. "Cyber Campaign Brief: Linked SWIFT-Themed Campaigns Deliver Keyloggers and Infostealers" February 2020. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--58
3. Infoblox Cyber Intelligence Unit. "Cyber Campaign Brief: Formbook Infostealer Campaigns Continue" September 2019. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--39
4. Infoblox Cyber Intelligence Unit. "Cyber Campaign Brief: Similar RTF Files Download Lokibot or Formbook" February 2019. http://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--27
5. Infoblox Cyber Intelligence Unit. "Cyber Campaign Brief: Formbook Information Stealer" January 2019. http://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--24

AZORult Infostealer

Author: Christopher Kim

Overview

From November 3 to 4, Infoblox observed fashion and beauty-themed malicious spam (malspam) campaigns that delivered AZORult information stealer (infostealer) via Microsoft Excel spreadsheets (XLS) with malicious macros. These spreadsheets used living off the land (LotL) techniques that abused preexisting software on the victim's machine in order to perform malicious tasks.

Customer Impact

The cybersecurity community first discovered AZORult infostealer in 2016.[1] The malware is often bought and sold in Russian dark web forums due to its data-stealing capabilities, which include the following:

- System information (e.g. system language, operating system version, user name and computer name)
- Bitcoin wallets
- Chat software message history
- Email and banking credentials
- Account information from file management software (e.g. FTP clients)
- Browser passwords, cookies and history

AZORult can also serve as a trojan downloader for other malware payloads.[2] Some versions of AZORult can even establish Remote Desktop Protocol (RDP) connections that allow the attacker to take complete control of the infected system.[3]

Earlier this year, malware campaigns used Coronavirus-themed lures to distribute this infostealer.[4]

Campaign Analysis

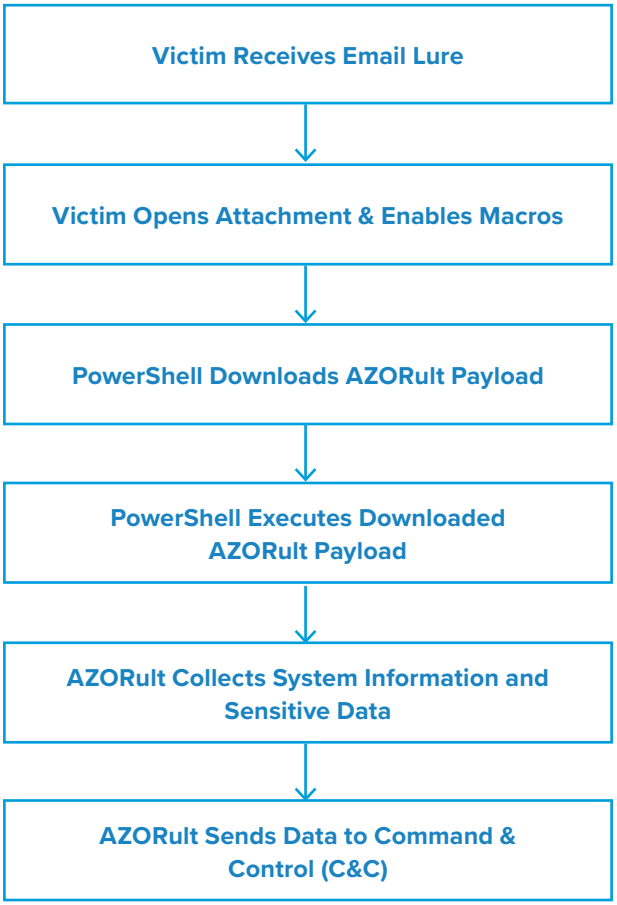
The campaigns we observed used fashion and beauty-themed lures with subject lines referencing design patterns. These campaigns also used spoofed email addresses to impersonate legitimate manufacturing businesses based in Portugal and Spain, including health and beauty supplier Mundinter as well as fashion manufacturer Dario Beltran. The email template used for the spoofed Mundinter emails was notably similar to a template used by a recent Agent Tesla campaign.[5] This type of similarity often occurs when different threat actors hire the same botnet to distribute malspam for both of their campaigns.

The emails contained brief and generic messages that encouraged recipients to open the malicious attachment *(FEBEL_List.xls or Patterns.xls)* and reply back for pricing information.

Attack Chain

When the user opened the XLS attachment and enabled macros, the macros in the attachment spawned PowerShell processes to download the AZORult payload from a website. All of the payloads used by the campaigns were hosted on open directories, one of which was publicly available since at least October 31.

The PowerShell command that downloaded the payload included additional parameters to evade detection and bypass security policies that could block script execution. When the malicious XLS macros ran this PowerShell command, it wrote the AZORult payload to a local file and executed it. AZORult then harvested system information and sensitive credentials. Lastly, AZORult exfiltrated this data by sending HTTP POST requests to its command & control (C&C) server.



Vulnerabilities & Mitigation

Infoblox recommends the following actions to reduce the risk of this type of infection:

- Subscribe to Infoblox's Threat Intelligence Feed for DNS Firewall. This feed contains known C&C domains that businesses can add to their Domain Name System (DNS) firewall for protection.
- Enforce strong password policies across all corporate systems and software.
- Apply strong email security solutions that offer spoofing controls such as Sender Policy Framework (SPF), Domain-based Message Authentication Reporting and Conformance (DMARC) and DomainKeys Identified Mail (DKIM).[6]
- Use password manager software to safely store sensitive credentials.
- Update threat signatures for web application firewalls (WAF) to detect malicious HTTP traffic.

Endnotes

1. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--29
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--17
3. https://success.trendmicro.com/solution/000146108-azorult-malware-information-kAJ4P000000kEK2WAM
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--63
5. https://www.pcrisk.com/removal-guides/18635-mundinter-email-virus
6. https://www.hhs.gov/sites/default/files/maldoc-information-stealer

Remcos RAT Malspam Campaign

Author: Jeremy Ware

Overview

During the week of November 9, we discovered a malspam campaign distributing the Remcos remote access trojan (RAT). The emails in this campaign carried malicious Microsoft Office documents that required the user to enable macros to execute the Remcos payload.

We previously reported on a similar Remcos campaign in July 2019. That campaign distributed Rich Text Format files (RTFs) and exploited the Microsoft Equation Editor remote code execution vulnerability.[1]

Customer Impact

Remcos is short for remote control and surveillance, and is a tool created by the security company Breaking Security, based in Germany.[2] However, it has been abused by threat actors in numerous malspam campaigns since Breaking Security began selling it in 2016, with pricing starting at 58 Euros.[3,4,5]

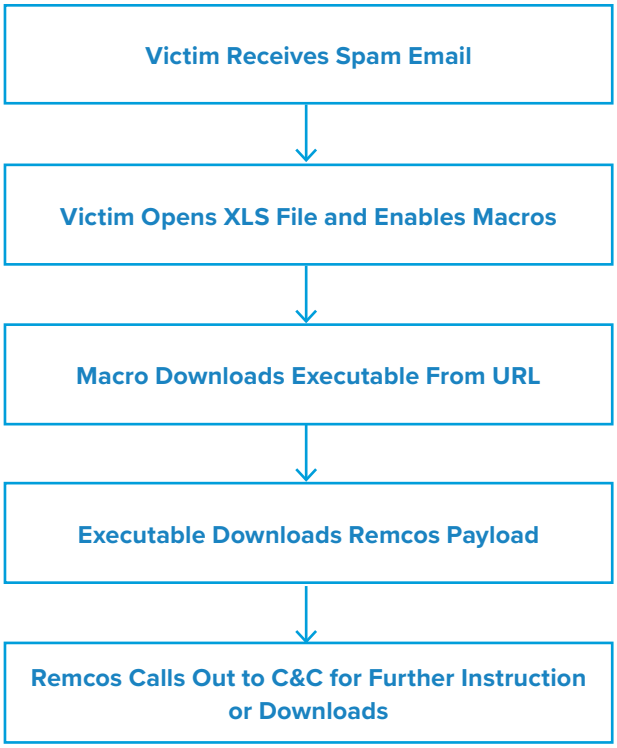
Remcos can control systems and cameras, act as a proxy for internet traffic, perform screen captures remotely, check browser cache and settings, and search files for password stores. It also includes a command-line interface (CLI) for full remote control.

Campaign Analysis

The campaign we observed uses lures mentioning purchase orders or lists in the subject line *(Re: Item request list from Medigas SRL)* and file name *(Item List 09112020.xls)*. The emails all had the same subject line, file name and sender data, and the body of the message was empty.

Attack Chain

When the victim opens the attached document, they are prompted to either enable macros or update the document. Esuerde.exe then begins to download, launches the Remcos payload (AddInProcess32.exe) and stores it in *C:\Users\admin\AppData\Local\Temp*. Next, the malware gathers data by checking stored credentials in files and reading browser cookies and cache settings. Remcos will continue to reach out to a command and control server (C&C) for further instructions or to receive additional payloads.



Vulnerabilities & Mitigation

The Remcos RAT is spread via spam email and takes advantage of Microsoft Office vulnerabilities. Infoblox recommends the following actions to reduce the risk of infection:

- Keep Microsoft Office security patches up to date.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.
- Do not open attachments from unfamiliar or unknown senders.
- Always be suspicious of unexpected emails, especially financial or delivery correspondence, documents or links.
- Regularly train users to be aware of potential phishing efforts and how to handle them appropriately.
- Convert attachments to another format, for example, converting Microsoft Office documents to PDF documents can be an effective method of neutralizing malicious content.
- Never enable macros, and do not configure Microsoft Office to enable macros by default.

Endnotes

1. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--32
2. https://attack.mitre.org/software/S0332/
3. https://www.fortinet.com/blog/threat-research/remcos-a-new-rat-in-the-wild-2
4. Given its usage in multiple malware campaigns, Cisco Talos conducted research on the German-registered company that builds and sells it - Breaking Security - and found them to be advertising on hacking websites. The software author claims many types of individuals visit such sites, not just hackers, and that he can shut down an instance of the tool if someone violates its terms and agreement.
5. As of 2018, the company also sold a crypter called Octopus Protector that was designed to allow software to bypass detection from anti-malware products by encrypting the software onto the computer's disk, thereby making it undetectable. https://blog.talosintelligence.com/2018/08/picking-apart-remcos.html

change image

Automotive-Themed Malspam Delivers Adwind RAT

Author: Victor Sandin

Overview

From November 12 to 13, Infoblox observed a malicious email campaign distributing the Adwind remote access trojan[1] (RAT) via a spoofed O'Meara Auto Group invoice using Microsoft Excel spreadsheets (XLS) with malicious macros.

Customer Impact

Adwind, also known as AlienSpy, jRat, Sockrat, etc., is one of the most widely-used cross-platform Malware-as-a-Service (MaaS) packages that threat actors can purchase for a fee.[2] Between 2013 and 2016, this malware targeted at least 443,000[3] private users, commercial and non-commercial organizations around the world. Adwind's capabilities include:

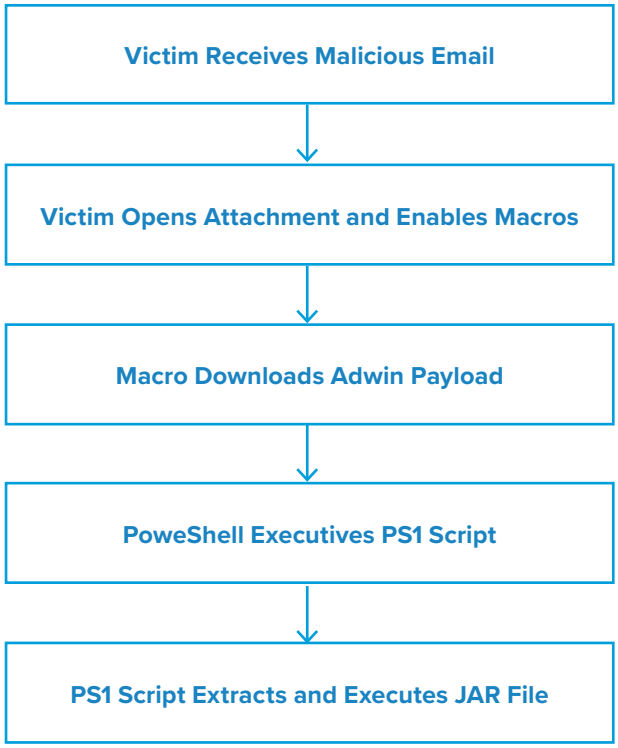
- Logging keystrokes
- Collecting system information
- Transferring data
- Controlling the victim's webcam
- Harvesting user credentials
- Recording sounds and taking screenshots

Campaign Analysis

In the campaign we observed, the threat actors sent emails with a subject and an email body of *Your Order confirmation # <XXXX>,* where the Xs represent a varied number of random digits. The emails also included an attached XLS file named *INVOICE # SPLXXXX*.

Attack Chain

When the user opens the attached XLS file and enables macros, the document reaches out to its command and control (C&C) server to download a PowerShell script and a ZIP file containing the Java Runtime Environment (JRE). It will then execute the PowerShell script using parameters that evade detection *(windowstyle hidden)* and bypass security filters *(ExecutionPolicy bypass).* This process decrypts and executes the JAR file containing the Adwind payload using the legitimate JRE that the malware downloads to *C:\User\bin\java.exe*. The PowerShell script also drops additional files to the user's AppData folder and adds an entry under the *Start Menu* to achieve persistence.



Vulnerabilities & Mitigation

Infoblox recommends the following to reduce the risk of this type of infection:

- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them especially if their subject is as generic as Invoice or Order confirmation.
- Never configure Microsoft Office to enable macros by default and be cautious if the file's only apparent contents are directions to enable macros.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.

Endnotes

1. https://securelist.com/adwind-faq/73660/
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--34
3. https://usa.kaspersky.com/resource-center/threats/adwind

Shathak Pushes IcedID in Japanese Malspam

Author: Eric Patterson

Overview

On November 20, security researcher Brad Duncan reported on a malicious spam campaign from the threat actor known as Shathak (a.k.a. TA551) to distribute the IcedID banking trojan via emails written in Japanese.[1]

We previously reported on a campaign in July wherein threat actors used a Valak downloader to deliver IcedID.[2]

Customer Impact

First discovered in 2017 by IBM X-Force researchers, IcedID (a.k.a. BokBot) is a modular banking trojan that uses man-in-the-browser attacks to steal banking credentials, credit card information and other financial data from victims.[3]

Campaign Analysis

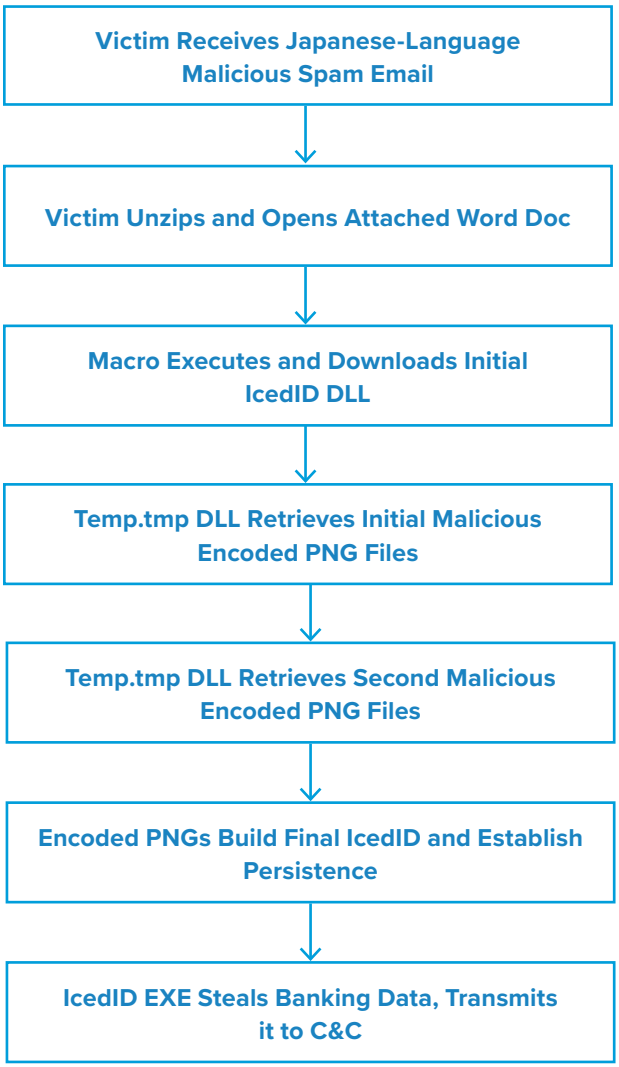
Based on the language in the email bodies, the threat actors appear to be targeting a Japanese-speaking audience, which could include individuals or organizations that are based in or conduct business with Japan.

The observed subject lures for this campaign are "*Re: Speech of welcome*" and both the message body and attached Microsoft Word document follow a template. The translated message body invites the recipient to "Please review that attached file" and provides a password to open the accompanying locked ZIP file. The compressed Word document within follows the naming convention *<single_word MM.dd.YY.doc> (e.g. adjure-11.20.20.doc)*.

Attack Chain

When the victim extracts the Word document and enters the password from the ZIP archive, the document displays a message that translates to "This file has been created in a previous version of Word[...] Please enable content." Once the victim does so, a malicious macro attempts to contact one of 11 domains to retrieve the initial IcedID installation dynamic-link library (DLL).

If successful, the malware downloads the DLL to *C:\Users\[username]\AppData\Local\Temp\temp.tmp*. The installer DLL then contacts additional malicious infrastructure ending in *.club* and *.cyou* to retrieve additional encoded Portable Network Graphs (PNG) image files.



IcedID uses these encoded PNG files to build the persistent DLL *Kaimei.dll* inside the victim machine. Once persistent, IcedID uses a series of web injections to redirect pertinent web traffic (e.g. login pages to financial institutions) to an IcedID proxy server. Here, the malware presents the user with a specially-crafted, malicious version of the desired website in an attempt to trick them into entering their banking credentials. Once the user inputs their login credentials, the threat actor stores and forwards the credentials to the legitimate banking website which allows the user to log in.

The threat actors are then able to use the stolen financial data or to sell it to others.

Vulnerabilities & Mitigation

Infoblox recommends the following actions to reduce the risk of this type of infection:

- Always be suspicious of vague emails, especially if there is a prompt to open an attachment or click on a link.
- If clicking on a link immediately initiates an attempt to download a file, that file is suspicious. Inspect it carefully.
- Never enable macros, and do not configure Microsoft Office to enable macros by default.

Endnotes

1. https://www.malware-traffic-analysis.net/2020/11/20/index.html
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--78
3. https://securityintelligence.com/posts/breaking-the-ice-a-deep-dive-into-the-icedid-banking-trojans-new-major-version-release/

Tools of the Trade White Paper: Distilling Campaigns in Spam

A graph-based sieve for email spam

Author: Dr. Renée Burton

Introduction

This paper introduces a technique used by the Infoblox Cyber Intelligence Unit to identify malicious campaigns from email spam. The methods described here allow us to automatically process large volumes of data to focus our resources for manual analysis. In this sense, the techniques act as a sieve for email spam. Specifically, we use bipartite graphs constructed from email metadata and compute the set of connected components within them to identify likely individual campaigns. We studied the results using these graph algorithms over an 18 month period and have developed a set of best practices for their use. We have not seen a similar practice published elsewhere, so will show the results of our research and describe the methods we used.

Infoblox security products leverage block lists to protect our customers and their network users from Internet threats at the Domain Name System (DNS) level. We create original content for these products from several types of source data, using a range of algorithms and techniques. One of those data types is email spam. While spam identification techniques have become much more effective and widely integrated into end-user mail systems, this type of email remains prevalent as spammers continually adjust to evade the protective measures. As a result, customers continue to receive spam in their inbox.

Cybercriminals leverage spam as a high volume, low cost means to infect victims with malware. They are then able to steal or hold for ransom personal and proprietary information, gain access to and control of system processes, as well as spread to other connected individuals or networks. Their strategy is similar to Internet advertising, in which the small likelihood that a user will click on a displayed ad created a $124.6B yearly industry.[1] Malicious actors target individuals, major corporations, organizations and governments alike. As a result, locating spam-based malware campaigns as quickly and as accurately as possible to prevent further damage is a critical capability for the cybersecurity community in our effort to protect others.

This paper will begin with background on malicious spam campaigns and the challenges of using spam data as a source for block lists. Our approach to addressing these challenges leverages the field of graph theory. We describe this technique and the terminology necessary to understand it in Section XX. Then we will walk through our results, and conclude with comments on other applications of graphs to threat intelligence derived from spam collection.

1. PwC, Internet Advertising Revenue Report, May 2020, https://www.iab.com/wp-content/uploads/2020/05/FY19-IAB-Internet-Ad-Revenue-Report_Final.pdf

Background

Malicious spam, often referred to as **malspam**, utilizes file attachments or embedded hyperlinks (URLs) to infect victims. The email recipient must either open the file or click on the URL, and often may need to enable macros or editing on their machine for the attack to continue. Threat actors use various types of lures, including spoofed documentation, promises of financial gain or threats of blackmail to trick victims into taking these steps. They gain access to the user's machine and often their private information by using lures that prey on people's hopes and fears, as well as inexperience with computer security. The consequences can be quite significant. One such example is the December 2019 Emotet attack that brought Frankfurt, Germany to a halt.[2] Organized thieves also leverage crises like the Coronavirus pandemic[3] or Black Lives Matter protests[4] as a means to lure victims and steal their financial information.

An effective lure is only the first step in the attack chain, which may involve several stages and can occur quickly or over a longer period of time. In modern malspam, the attachments themselves generally serve to download further malware. This multi-stage process reduces the likelihood of stopping the malware infection through automated detection, and also allows the malware distributor to conduct checks on the victim's location or system configuration before proceeding. Malware delivered via email ultimately reaches out through the victim's network to its command and control (C&C) endpoint(s). The C&C domain names, IP addresses and URLs are referred to as indicators of compromise (IOCs). Recovering these IOCs for use in block lists is the ultimate goal of this research.

However, the massive volume of email spam, as well as the staged approach of the threat actors and their constant adaptation to avoid detection make it difficult to isolate IOCs. Traditional approaches leverage algorithms, both heuristic and machine learning, to identify suspicious code or content in websites. In some cases, automation is able to definitively determine whether a given attachment or URL is malicious, but more often it will lead to large quantities of generically suspicious emails requiring manual review. There are not enough human resources to manually evaluate all of these results.

As a result, we are left with large volumes of complex data and limited resources to locate the malicious behavior within it. By applying methods taken from the long-established scientific fields of graph theory and social network analysis, we created a workflow that allows us to automatically group together emails that are likely part of the same spam campaign. We use this as an initial filter and then apply more traditional methods of threat intelligence to the results. This multi-step process allows us to focus our resources and harvest IOCs more efficiently. In the next two sections, we define terminology and detail our technique.

Terminology

A **graph** is a mathematical representation of connections between different items called nodes within a set. Two nodes are connected by an **edge** if they share some attribute or feature. Graphs abound in our everyday life, and we intuitively incorporate them into our decision processes. Some familiar examples include:

- Social media leverages connections between individuals, creating a network in which nodes are representations of people, and edges represent relationships such as friendship, readership, or common interests.
- Contact tracing in viral outbreaks creates a graph in which nodes are individuals and edges represent contact.

2. Kaspersky ICS-CERT, German cities under attack by Emotet botnet, 24 December 2019, https://ics-cert.kaspersky.com/news/2019/12/24/emotet-attacks-german-cities/
3. US Center for Disease Control, COVID-19-Related Phone Scams and Phishing Techniques, 3 April 2020, https://www.cdc.gov/media/phishing.html
4. E. Patterson, BLM Themed Malspam Delivers Trickbot Trojan, 1 July 2020, https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--77

Graphs in one form or another have long been used in investigations. The oldest, and among the most famous is the work by John Snow[5] in identifying the source of London's cholera outbreak from 1853 to 1854. This study influenced not only epidemiology, but the fields of network analysis and graph theory. Evolutions of Snow's original results have been produced over 150 years later including work by Shiode[6] to further visualize the distribution of victims. The social sciences and epidemiology originally dominated the use cases for graphs, which were most often hand constructed and easily interpreted. The advent of computers and the capability to conduct large-scale processing opened the door for areas of mathematics and computer science to process and visualize extremely complex networks.

There are numerous types of graphs. The techniques described in this paper leverage undirected bipartite graphs. A graph is **undirected** when there is no inferred directional relationship between the nodes. Undirected graphs are most easily understood as the opposite of directed graphs, in which an edge between two nodes has some specific relationship. For example, a graph consisting of email addresses representing email sent between parties is directed if the edges are interpreted as node A sent email to node B, but node B may not have necessarily sent email to node A. Each edge in such a case represents a directional relationship.

If a graph is constructed with nodes that split into two distinct sets, and edges only exist between the sets, the graph is considered a **bipartite** graph. This is sometimes referred to as a **bigraph**. For example, a graph constructed from email in which the nodes are the set of sender addresses and the set of subject lines, and edges represent an email from the sender with that subject, is a bipartite graph. Edges in a graph can be assigned a weight to indicate frequency of a relationship or importance. In our example, the **weight** of an edge might be the number of emails from the sender with a given subject line.

Two nodes are considered **connected** if there is an edge between them. A **connected component**, often shortened to component or **cluster**, is a subset of the graph in which all of the nodes are connected by edges. Within a connected component, any node can be reached from any other node by traversing edges. The **size** of a component here is defined as the sum of the weights of all of its edges.

Email metadata includes the headers and envelope associated with an email and its transmission across the Internet. This metadata contains structured and unstructured data related to the original email, along with a log of the steps taken for it to reach the destination. The actual communication within the email is considered the body. The headers and envelopes are themselves quite complex, and for the purposes of paper, we will restrict the discussion to commonly recognized fields, e.g., the subject, the sender's IP address, attached filenames, etc.[7, 8]

We define a malspam **campaign** to be a set of emails sent by a threat actor, through either the use of a spambot or a directly controlled infrastructure. We classify malspam campaigns as being limited in both time and content. The emails in a campaign may contain several topics, but share other features such as malicious attachments, or focus on a single theme, such as shipping notifications or current events with variations in other features.

Technique

To isolate spam campaigns, we create an undirected bipartite graph from email metadata. Each connected component within the resulting graph represents a set of emails that are likely all part of a single campaign. Treating each component as related allows us to focus our subsequent threat intelligence processes onto representatives of each component, as well as prioritize our resources based on the size of campaign or some other feature of the graph.

---

5. The John Snow Archive and Research Companion, https://johnsnow.matrix.msu.edu/index.php
6. S. Shiode, Revisiting John Snow's Map: network-spatial demarcation of cholera area, February 2012, https://www.tandfonline.com/doi/full/10.1080/13658816.2011.577433
7. wikipedia.org, Simple Mail Transfer Protocol, https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol, https://tools.ietf.org/html/rfc5321
8. wikipedia.org, Internet Message Format, https://en.wikipedia.org/wiki/Email#Internet_Message_Format, https://tools.ietf.org/html/rfc5322

These graphs can be computed over varying time intervals. We have found that a window of three to five days is very effective in identifying complete and accurate campaigns. We use longer timeframes to study the threat landscape, and shorter intervals to quickly isolate campaigns for the purpose of extracting threat indicators.

Additionally, there are a large number of combinations within email metadata to use for nodes within the graph. We found the optimal choice to be somewhat dependent on the exact nature of the email collection. For example, the use of subject lines and filenames works well in cases where the email contains file attachments.

Illustration of Results

We studied the effectiveness of these techniques over an 18 month period. To demonstrate the results, we will use a set of over 21,000 emails containing attachments from 18 to 24 December 2019. We constructed an undirected bipartite graph with nodes drawn from the email subject lines and the attachment filenames. In this dataset, unique attachments are in direct correlation with filenames, meaning every filename represents a distinct file attached to the email. While not always the case, this is a dominant feature we have consistently observed in spam over time.

The initial graph has 866 components, many of which may contain a single email. To reduce noise, we remove components with a size less than five. This reduces the total number of nodes, thereby reducing the number of components to 101. As an immediate result, assuming the components capture campaigns well, we have reduced the number of items needing review by 99.5 percent, from the original 21,000 emails to a single representative email from each cluster. As shown in Figure 1 below, by coloring the nodes consistent with their type, we can also gain an overall understanding of the emails in this dataset. In particular, notice two large clusters dominated by the color green, indicating that they have a very large number of filenames and a smaller number of distinct subjects. In contrast, three large sets are loosely connected and are characterized by a large number of subject lines.

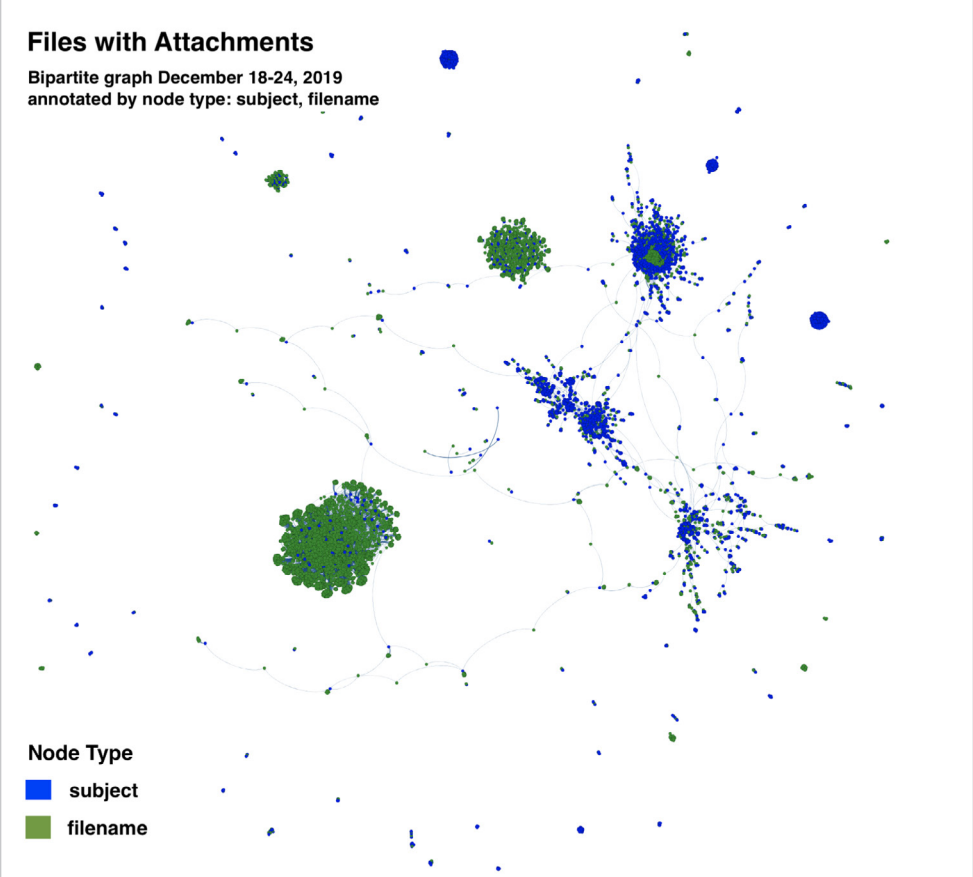


Figure 1. A bipartite graph generated from spam December 18-24, 2019.

If we color each node in the graph instead by the associated connected component, we see that the vast majority of emails are found in a handful of components. This allows us to focus our analytic resources on campaigns with larger impacts. In particular, as shown in Figure 2 below, we find that the loosely connected emails above are all part of an Emotet campaign that lasted for much of the week.

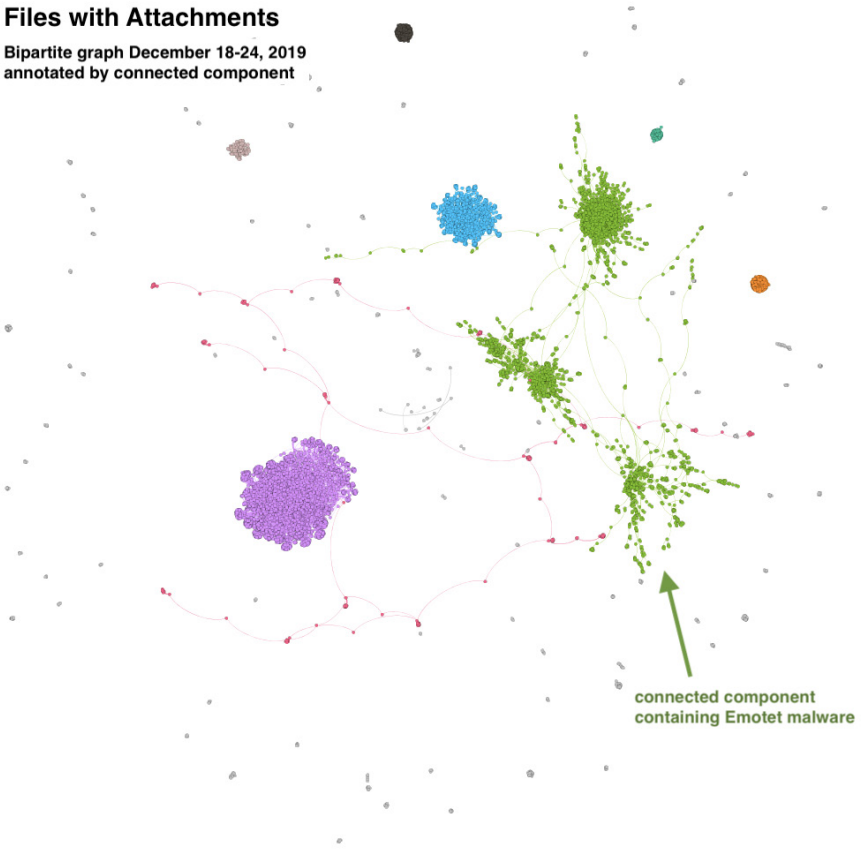


Figure 2. The same bipartite graph as in Figure 1 colored by connected components.

If we isolate our review to the large set of malicious emails sent by the threat actor behind Emotet, shown in green in the Figure 2, we can demonstrate a number of other features of our technique. First we compare the difference between the graph resulting from one, three and five days of data, as shown in Figures 3 through 5. This illustrates two advantages of increasing the time frame used; disparate components are drawn together over time, and the larger data set includes a more complete set of the actor's activity.

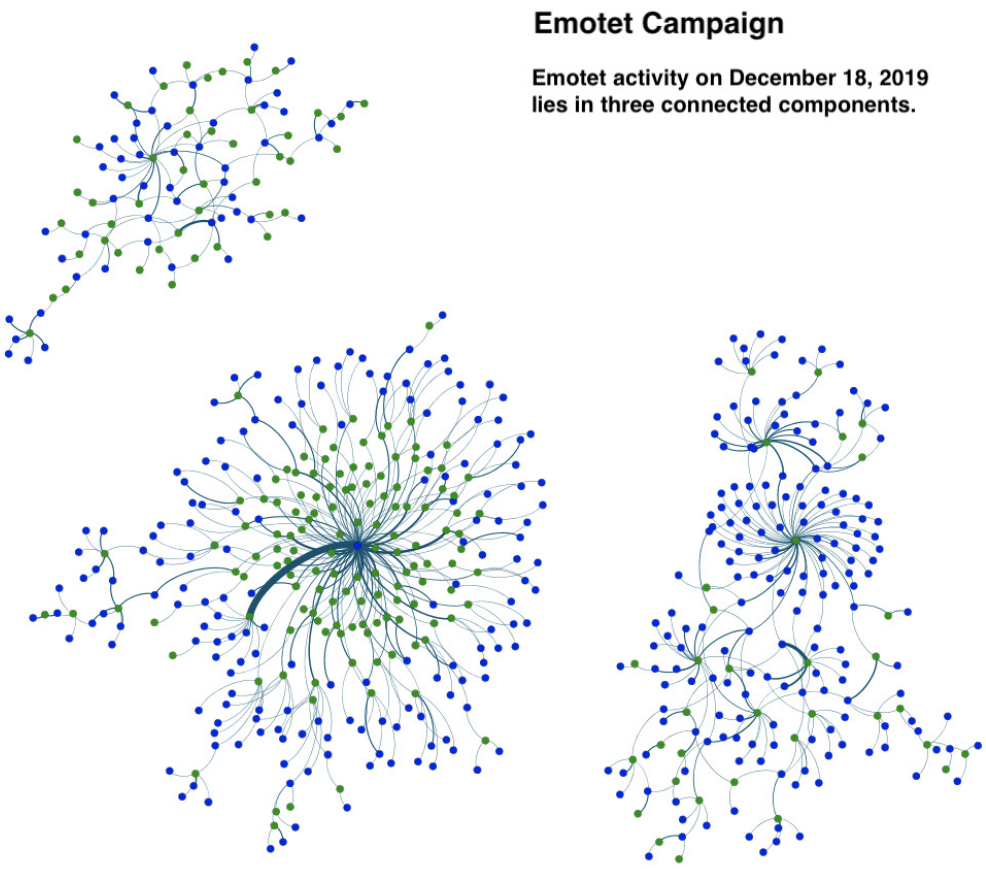


Figure 3. An Emotet campaign from December 18, 2019. This is a subgraph of the graph shown in Figure 1.

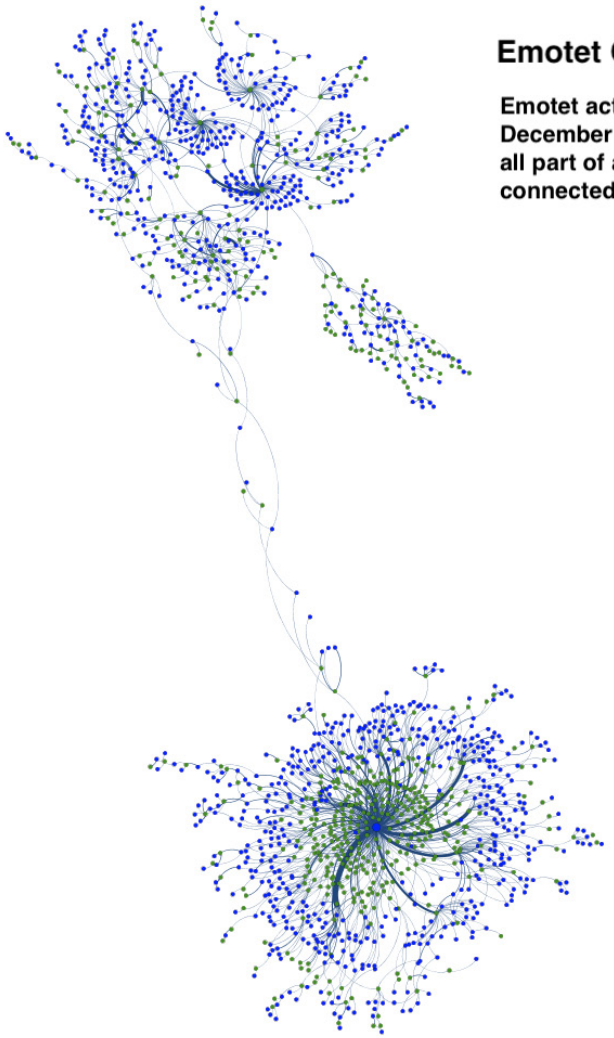


Figure 4. An Emotet campaign as observed over December 18-20, 2019. This is a subgraph of the graph shown in Figure 1.

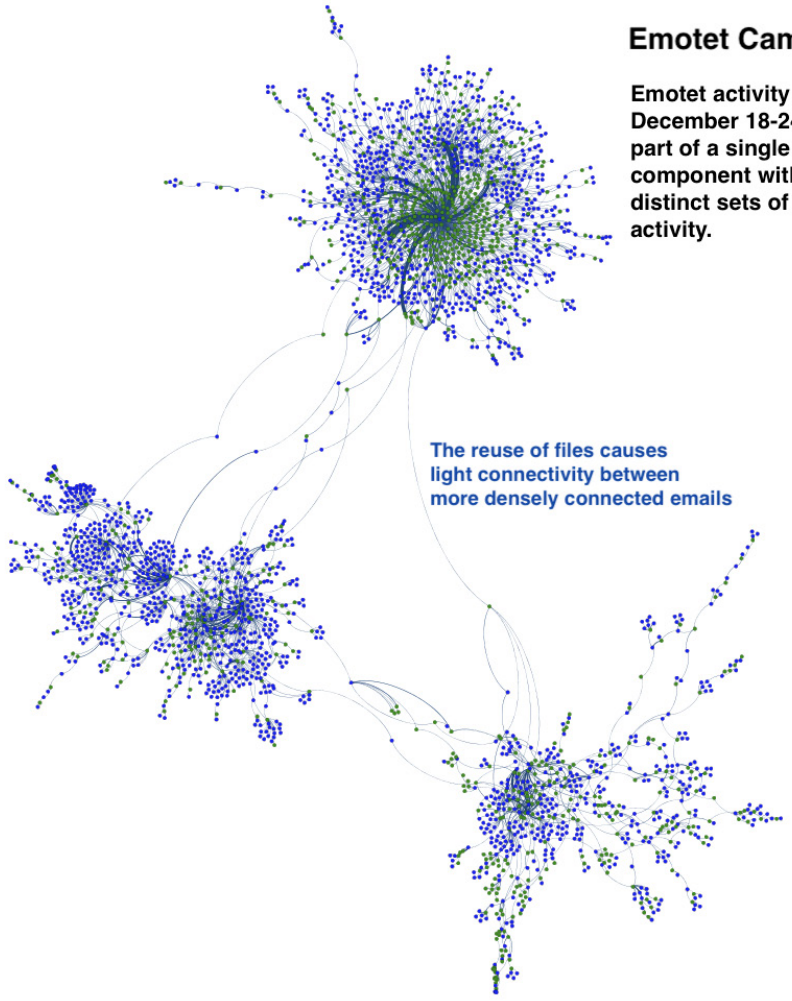


Figure 5. An Emotet campaign as observed during December 18-24, 2019. This is a subgraph of the graph in Figure 1.

Another advantage of the graph technique is that it correlates activity not fully visible in open source intelligence (OSINT) sources. In Figure 6, we can see a subset of the Emotet campaign and the relative proportions of inclusion in VirusTotal, a popular repository of file classifications by various anti-virus vendors. The use of the connected component as an initial filter allows us to associate many more files with Emotet's activity than through OSINT alone.

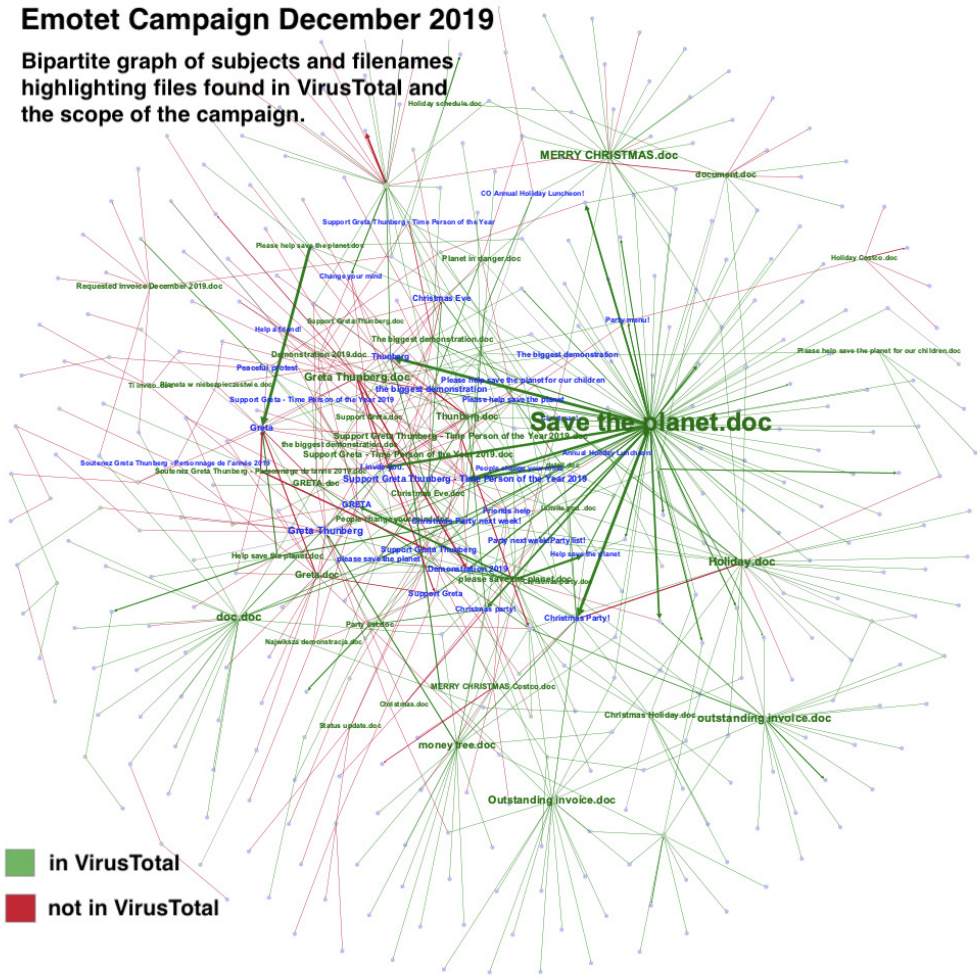


Figure 6. An Emotet campaign annotated by the presence of the file in the public repository VirusTotal.

Conclusion

Our primary use case for graph techniques is to easily identify malspam campaigns for more reliable, efficient indicator extraction. To this end, the graph must be constructed such that the components are, as much as possible:

- pure, or correct, campaigns
- complete campaigns.

In general terms, the former goal is easier than the latter. While we evaluated a wide variety of graph constructions for this purpose, we have found the use of bipartite graphs to be the most effective. In addition to isolating campaigns, we have used these graphs for other purposes, such as providing insight into the overall threat landscape. These techniques led to the discovery of the malicious spam actor, WordyThief,[9] who distributes malware that steals personal data from victims.

We recommend the following practices based on our results:

- Separate data into categories that can be analyzed independently. For example, these categories could be based on whether attachments exist, and of what type, or whether the emails contain embedded URLs.
- Within a category, perform statistical analysis on the primary fields identified by the subject matter experts as relevant to campaigns. In particular, two fields that are of one-to-one correspondence will not add value to your graphs, and only one should be used. Fields that contain the most diversity are more likely to be helpful in campaign isolation.
- Create graphs over multiple days to capture accidental transitions made by the threat actor and to visualize the full scope of malicious activity.

9. Burton, Tymchenko, Sundvall, Hoang, Mozley, Josten; Wordy Thief: A Malicious Spammer, eCrime2020 conference proceedings, to appear November 2020

December 2020

Threat Reports &

Cyberthreat Alerts

Malspam Spoofing Document Signing Software Notifications Deliver Hancitor Downloader and Follow-On Malware

Author: James Barnett

Overview

Between November 23 and December 8, Infoblox observed multiple malicious spam (malspam) campaigns that all used DocuSign-themed lures to entice users to download and open Microsoft Word documents with malicious macros that install embedded copies of the Hancitor trojan downloader.

Customer Impact

Hancitor is a trojan downloader that targets businesses and individuals around the world. It is distributed via malspam sent by compromised servers in many countries, including the United States, Japan and Canada. These malicious emails mimic notifications from legitimate organizations to entice the user to download a weaponized Microsoft Office document.

We wrote about a previous Hancitor campaign in April 2020.[1] While many of Hancitor's core characteristics have remained the same, this recent series of campaigns includes a slightly more complex attack chain and delivers different types of malware payloads after establishing the initial Hancitor infection.

Campaign Analysis

The emails in these campaigns used a DocuSign lure to entice targets into opening links in the messages. The subject lines of the messages indicated that the target had a pending invoice or notification from DocuSign. Each email contained an embedded link leading to a Google Docs file.

Attack Chain

When the victim clicks the link in the initial Hancitor malspam message, they are taken to a published Google Docs file. This file contains a message that states "Previewing is disabled" and instructs the user to click another link to download the document. When clicked, this link downloads a Microsoft Word document containing malicious macros.

When the victim opens the downloaded Word document, it displays a message instructing the viewer to enable content. If the victim does so, the malicious macros in the document will execute. These macros then extract and execute the Hancitor payload dynamic link library (DLL) embedded within the Word document, thus establishing the initial Hancitor infection.

Once Hancitor infects the victim's system, it sends some basic information about the system to one of its three hardcoded command and control (C&C) servers. The server responds with further instructions that direct Hancitor to download and execute one or more additional malware payloads. In these campaigns, Hancitor delivered two additional payloads.

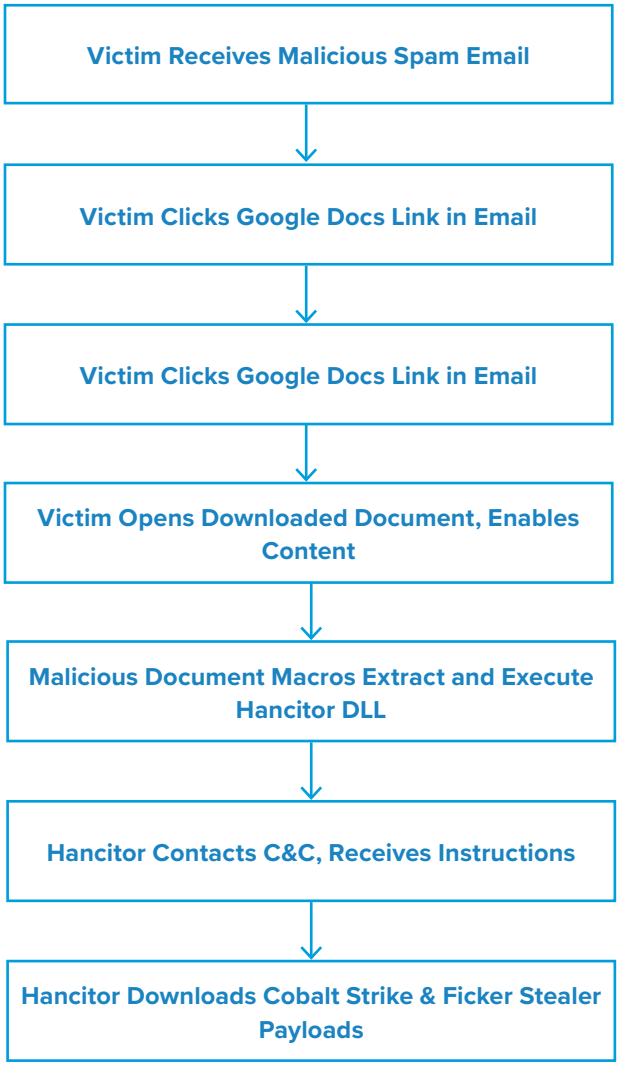
The first additional payload was Cobalt Strike, a legitimate penetration testing tool that has become increasingly popular amongst threat actors. Its features include infostealer capabilities such as keylogging, exploits that can leverage system vulnerabilities to facilitate additional attacks, and various methods to help conceal its activity on both the infected system and the victim's network.[2]

The second follow-on payload was Ficker Stealer, a relatively new Malware-as-a-Service (MaaS) infostealer that was initially identified in August 2020.[3] According to the author of Ficker Stealer, the malware is capable of stealing web browser passwords, cryptocurrency wallets, FTP) client information, credentials stored by Windows Credential Manager and session information from various chat and email clients.[4]

Vulnerabilities & Mitigation

Hancitor uses several advanced detection countermeasures to bypass antivirus and firewall-based security. The best way for users to protect themselves from Hancitor is to be wary of links in incoming emails.

- If a well-known company provides a link, that link should generally point to the company's domain (e.g. "http://fedex[.]com" if the sender is FedEx).
- Be suspicious of links that immediately attempt to download a file when clicked.
- Do not enable macros in a Microsoft Office attachment, especially if the file's only apparent content is a message with instructions to enable macros.



Endnotes

1. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--69
2. https://www.cobaltstrike.com/features
3. https://twitter.com/Cyber_Bolo/status/1294576137495023616
4. https://twitter.com/3xp0rtblog/status/1321209656774135810

AveMaria RAT Malspam Campaign

Author: Yadu Nadh

Overview

Between December 2 and 7, Infoblox observed a malicious email campaign distributing the AveMaria remote access trojan (RAT). In this campaign, threat actor(s) used subjects referencing text message logs to lure users into opening a malicious Rich Text Format (RTF) file attachment that was disguised as a Microsoft Word document (DOC).

We previously reported on an AveMaria campaign in April 2019 that used shipping lures and contained similar malicious DOC files.[1]

Customer Impact

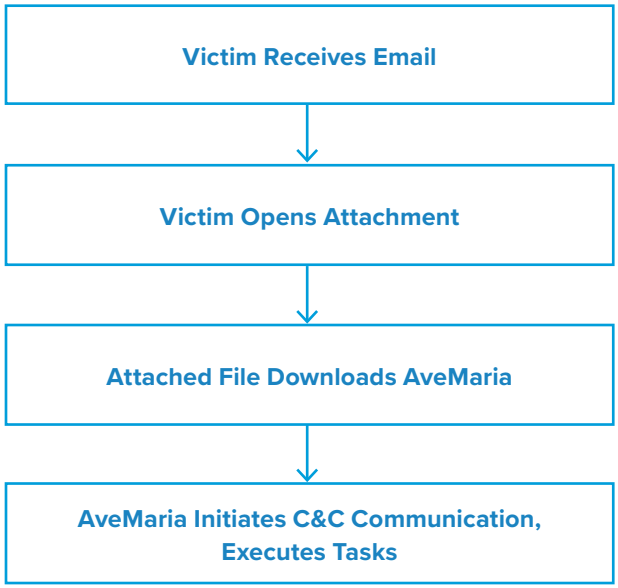
Cyber security company, Yoroi, first reported on AveMaria in early 2019.[2] It is a RAT with information-stealing abilities and has often been distributed via malicious email campaigns. The malware's other capabilities include communicating with a command and control (C&C) server, downloading and executing additional malware, bypassing Windows User Access Control (UAC) and others.

Campaign Analysis

In this campaign, threat actor(s) sent emails with the subject line *SMS Logs-Nov 2020*. The body of the emails instructed the recipients to verify the payment that was sent.

Attack Chain

When the victim opens the attached RTF, it exploits CVE 2017-11882 to download and run an AveMaria executable, infecting the victim.[3] Once this is complete, AveMaria will reach out to its C&C to initiate communication and execute any post-infection tasks, such as harvesting credentials and transmitting them back to the server.



Vulnerabilities & Mitigation

Malicious spam attachments that exploit a known vulnerability are the primary infection vectors for AveMaria. Infoblox recommends the following actions to reduce the risk of this type of infection.

- Keep computers and all endpoints up-to-date with the latest security patches to block known vulnerabilities that threat actors could target.
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.
- Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.

Endnotes

1. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--11
2. https://yoroi.company/research/the-ave_maria-malware/
3. https://portal.msrc.microsoft.com/en-US/security-uance/advisory/CVE-2017-11882

Cyberthreat Advisory: SolarWinds Supply Chain Attack

change image

Author: Nathan Toporek

Executive Summary

On December 13, FireEye publicly disclosed information about a supply chain attack affecting SolarWinds' Orion IT monitoring and management software.[1] This attack infected all versions of Orion software released between March and June 2020 with SUNBURST malware, a sophisticated backdoor that uses HTTP to communicate with attacker infrastructure. The threat actor(s) employed several advanced tactics, techniques and procedures (TTPs) that indicate a nation state and/or an advanced persistent threat group (APT) carried out the attack. Although some companies have suggested attributing the attack to a known APT, many organizations, including FireEye, are resisting early attribution.

Analysis

SUNBURST Backdoor

The *SolarWinds.Orion.Core.BusinessLayer.dll* file is a digitally-signed part of Orion software that contains the SUNBURST backdoor and is installed during either a routine software update or during initial SolarWinds Orion installation. Between twelve and fourteen days after the initial compromise, SUNBURST will create a unique pipe that ensures only one instance of itself runs on an infected machine. It will then read and modify the *SolarWinds.Orion.Core.BusinessLayer.dll.config* file's appSettings field to repurpose it for a persistent configuration. SUNBURST then checks that it is a part of the victim's domain, generates a userID and reads an initial value from its configuration.

SUNBURST will iterate over a known blocklist of services and set the associated registry key values to four to disable these services. Once it disables all blocklisted services, SUNBURST will resolve the domain *api[.]solarwinds[.]com* to test for, and confirm, internet connectivity. SUNBURST then uses a domain generation algorithm (DGA) to determine and resolve a random subdomain of a malicious second-level domain (SLD). It is important to note that in some cases, the actor(s) behind SUNBURST specifically tailored their infrastructure to different victims.[2]

SUNBURST will wait between each DGA resolution; in some cases, it will wait between one and three minutes; in others, 30 to 120 minutes; and on error conditions, it will wait between 420 and 540 minutes. If a DNS response's A record is within a known set of classless inter-domain routing (CIDR) blocks, SUNBURST will modify its configuration to prevent future execution before terminating itself.

When SUNBURST retrieves a CNAME record in its response, it will start an HTTP thread that manages command and control (C&C) communications. This thread will wait a configurable amount of time (at least one minute) between requests. It uses the HTTP GET or HEAD methods when requesting data from the C&C, as well as the HTTP POST or PUT methods to send data in the form of a JSON blob to the C&C. Responses appear as benign XML data, but the data has commands encoded in both Globally Unique Identifier (GUID) data and other hexadecimal (HEX) data.

TEARDROP & BEACON Malware

FireEye reported that SUNBURST delivered multiple payloads, and on at least one occasion, they observed it delivering TEARDROP – a unique, memory-only dropper. Actors likely used TEARDROP to deploy Cobalt Strike's BEACON malware.

Firefox Malware

The actor(s) behind this attack exercised highly-sophisticated operational security (OPSEC) while carrying out operations against their victims. They:

- Ensured hostnames matched the victim's environment,
- Used IP addresses in the same country as the victim,
- Used separate credentials for remote access and lateral movement, and
- Temporarily overwrote files with malicious utilities to later rewrite the original file contents.

These actor(s) also leveraged two additional variants of malware: COSMICGATE and SUPERNOVA. COSMICGATE is a credential stealer written in PowerShell, and SUPERNOVA is a Windows .NET program that acts as a legitimate SolarWinds HTTP handler.

Prevention and Mitigation

FireEye recommends upgrading to Orion Platform release **2020.2.1 HF 1** if possible. If an organization is unable to upgrade to this version of Orion, they recommend taking the following actions:

- Disconnect SolarWinds servers from the internet and isolate them, or restrict access from SolarWinds servers if this is not possible.
- Rotate credentials to accounts that have access to SolarWinds servers and/or infrastructure.
- Review network configurations created by SolarWinds, looking for anomalies.

Microsoft's Security Response Center has also provided important steps customers should take to protect themselves from the recent nation-state activity.[3]

In addition to this, the US Department of Homeland Security (DHS) recommends taking the following actions ***once all known malicious accounts and persistence methods have been removed:***[4]

- Assume all hosts monitored by SolarWinds Orion software are compromised.
- Rebuild hosts monitored by SolarWinds Orion software.
- Take actions to remediate Kerberoasting;[5] engage with third parties experienced in dealing with APTs as needed.

Endnotes

1. "Highly Evasive Attacker Leverages SolarWinds Supply Chain ...." Dec. 13 2020, https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html. Accessed Dec. 14 2020.
2. "SANS Emergency Webcast: What you need to know about the ...." Dec. 14 2020, https://www.sans.org/webcasts/emergency-webcast-about-solarwinds-supply-chain-attack-118015. Accessed Dec. 14 2020.
3. Microsoft Security Response Centre – https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/
4. "cyber.dhs.gov – Emergency Directive 21-01." Dec. 13 2020, https://cyber.dhs.gov/ed/21-01/. Accessed Dec. 14 2020.
5. See – https://attack.mitre.org/techniques/T1558/003/

LokiBot Campaign Uses Microsoft Office Exploit

Author: Darby Wise

Overview

On December 9, Infoblox observed a malicious email campaign exploiting CVE 2017-11882[1] to distribute LokiBot malware. This campaign used purchase order-themed lures to entice victims into downloading malicious Microsoft Excel (XLS) files.

We have previously written several reports on LokiBot, including campaigns that used Coronavirus-themed lures, NGROK tunneling to download payloads, and malicious RTF files to infect victims.[2,3,4]

CVE 2017-11882, a stack buffer overflow vulnerability in the Microsoft Equation Editor, is an exploit commonly used by threat actors. This past week, we observed a number of similar campaigns that use this CVE in their attack chains and distribute malware such as Agent Tesla, Formbook and AveMaria.

Customer Impact

LokiBot is a popular information stealing trojan first observed in 2015 and is frequently distributed through malspam campaigns. It is capable of harvesting the victim's login credentials, cryptocurrency wallets and other sensitive information through various methods such as keylogging. The malware then reports the stolen information to a command and control (C&C) server.[5]

LokiBot is also capable of establishing backdoors that enable the attacker to install additional payloads.

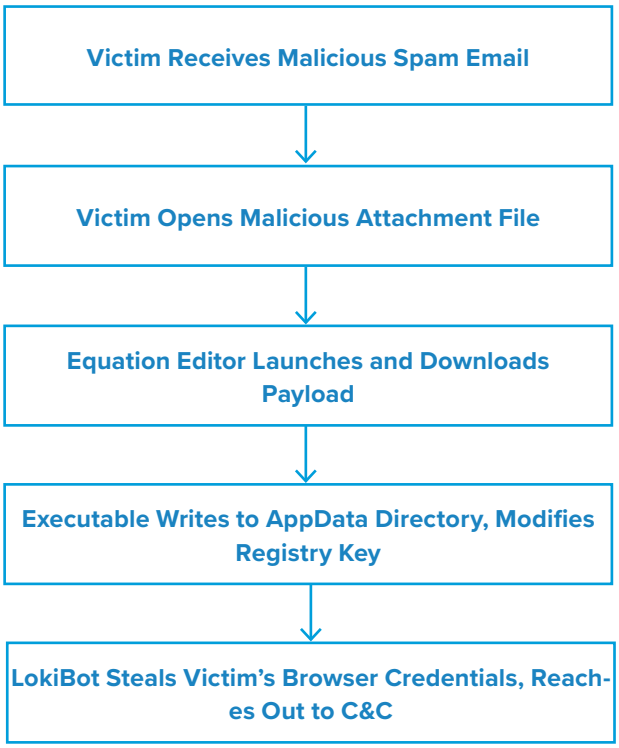
Campaign Analysis

Threat actors used a common malspam theme referencing purchase orders in this campaign. Email subjects included *Purchase Order Confirmation for December 1st Lot and ORDER CONFIRMATION*. All of the emails contained an attached XLS file named Purchase Order Confirmation.xlsx. The email bodies were either empty or contained a short greeting such as "Dear All" and "Good day."

Attack Chain

When the victim opens the XLS file attachment, it automatically exploits CVE 2017-11882 to download and run the LokiBot payload (*vbc.exe*).

To maintain persistence, the executable writes itself into the user's AppData directory and modifies a registry key. Finally, the malware begins to steal the victim's browser credentials, along with other personal data, and transmits it to its C&C server.



Vulnerabilities & Mitigation

Malicious spam attachments are the primary infection vector for LokiBot. Infoblox recommends the following actions to reduce the risk of this type of infection.

- Always be suspicious of unexpected and vague emails and unknown senders.
- Do not open attachments that are unexpected or from unfamiliar senders.
- Exercise additional caution when unexpected messages or attachments have commonly used themes such as shipping or financial documents or advice.
- Verify important or potentially legitimate attachments with the sender via alternative means such as a phone call or separate email to a known contact.

Endnotes

1. https://nvd.nist.gov/vuln/detail/CVE-2017-11882
2. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--62
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--16
4. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--27
5. https://us-cert.cisa.gov/ncas/alerts/aa20-266a

Encrypted Excel Files Drop Abracadabra Trojan

Author: Victor Sandin

Overview

From December 13 to 14, Infoblox observed a spam email campaign distributing a trojan known as Abracadabra[1] via an encrypted Microsoft Excel spreadsheet (XLS) with malicious macros. In this campaign, threat actor(s) used an email subject referencing an overdue invoice to lure users into opening the malicious attachment.

Customer Impact

Abracadabra is a malware variant that was first discovered in April 2020. Threat actors deliver this malware as an encrypted Excel file that when opened, automatically begins decryption once Excel uses the embedded default password, *VelvetSweatshop*.[2] This method of distribution allows the malware to bypass signature-based antivirus detectors because Excel does not decrypt the payload until the user opens the file.

Abracadabra's capabilities include maintaining persistence, process hooking and communicating with its command and control (C&C) server to infect victims with malware.

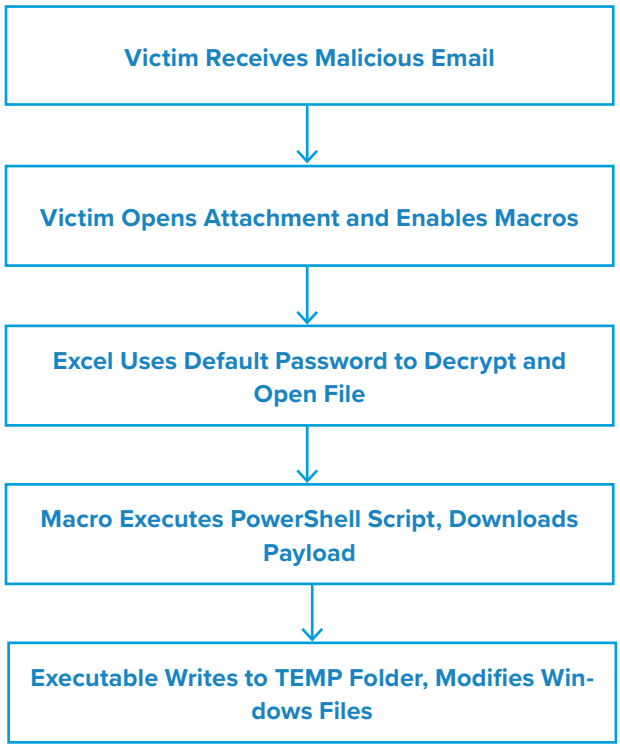
Campaign Analysis

In this campaign, the threat actors used the sender address *sales@webmail-expert[.]com*. The subject line (*Overdue Invoice*) and attached XLS file (*Overdue Invoice.xls*) reflect a lure theme that is common in malspam campaigns.

Attack Chain

When the user opens the attached XLS file and enables macros, Excel decrypts the file using the default password *VelvetSweatshop* and executes a malicious VBA macro. This macro invokes a PowerShell script that downloads a portable executable (PE) file with the Abracadabra payload from the C&C, which is on a Discord CDN server. It then moves the PE file to the user's TEMP folder, changes its permissions and executes the payload.

To maintain persistence, the executable modifies several Windows dynamic-link libraries in the user's .NET Framework folders.



Vulnerabilities & Mitigation

Infoblox recommends the following to reduce the risk of this type of infection:

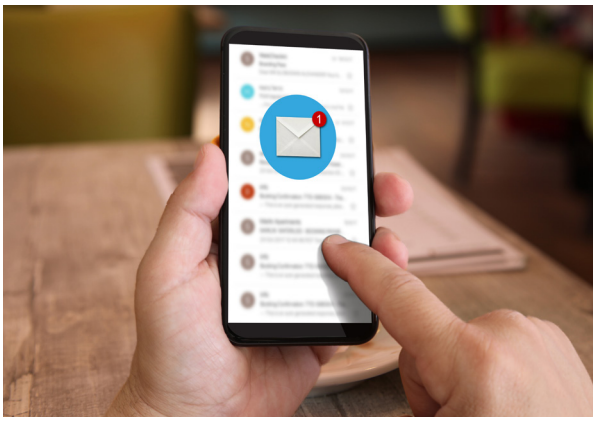
- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.
- Configure Microsoft Office to disable macros by default and be cautious if the file's only apparent contents are directions to enable macros.
- Use a layered defense for the best protection against malware.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.

Endnotes

1. https://www.helpnetsecurity.com/2020/09/25/malware-detections-q2-2020/
2. https://meindertjan.com/2012/08/22/microsoft-offic-and-its-velvetsweatshop-password-protected-files/

Malspam Sender Spoofing Indian Companies Drops Agent Tesla Keylogger

Author: Victor Sandin



Overview

Between December 13 and 14, Infoblox observed a malicious spam (malspam) email campaign distributing Agent Tesla keylogger[1] via a Microsoft Excel spreadsheet (XLS) with malicious macros. In this campaign, threat actor(s) sent emails spoofing communication from Gopaldas & Sons (also Gopal Das & Sons, both of which represent several large companies in India).

Customer Impact

Agent Tesla is a credential-stealing malware that was first discovered in 2004. It is sold through a subscription-based license on its official website, and according to Threatpost, it has been one of the most popular malware variants in 2020.[2] Agent Tesla's main capabilities include:

- Keylogging
- Harvesting configuration data and credentials from VPN, FTP and email clients, as well as from web browsers
- Collecting system information
- Transmitting stolen data to its command and control (C&C) via SMTP or FTP
- Evading detection and analysis through strong cryptography protocols

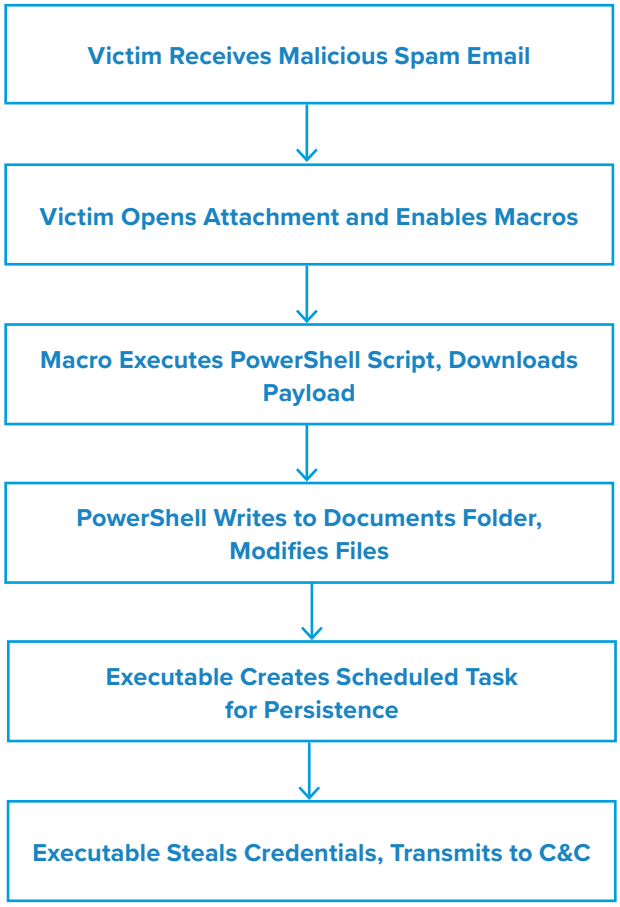
Campaign Analysis

In this campaign, the threat actor(s) distributed emails that impersonated a Gopaldas & Sons purchasing manager with the sender address *lv@gopaldas-sons[.]com* and subject line *Tool kit Lugdivine new order*. The email bodies claimed that the attached file, *RFQ Gopaldas selection.xls*, contained a compiled collection of their products.

Attack Chain

Similar to previous Agent Tesla campaigns,[3] when the user opens the attached XLS file and enables macros, Excel executes a malicious VBA macro. This macro invokes a PowerShell script that downloads the Agent Tesla payload from a controlled C&C server, drops it to the user's Documents folder and executes it.

To maintain persistence, the executable creates a scheduled task that runs every time the system boots up. Finally, it collects credentials from the computer and transmits them to the threat actor's C&C server using SMTP protocol.



Vulnerabilities & Mitigation

Infoblox recommends the following to reduce the risk of this type of infection:

- Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them. Especially if they use commonly-used themes such as shipping or financial documents or advice.
- Configure Microsoft Office to disable macros by default and be cautious if the file's only apparent contents are directions to enable macros.
- Configure firewall rules properly to block unusual traffic.
- Verify important or potentially legitimate attachments with the sender via alternative means (e.g., by phone or in person) before opening them.

Endnotes

1. https://labs.sentinelone.com/agent-tesla-old-rat-uses-new-tricks-to-stay-on-top/
2. https://threatpost.com/agent-tesla-spyware-tricks-arsenal/158284/
3. https://insights.infoblox.com/threat-intelligence-reports/threat-intelligence--65

change image

Cyberthreat Advisory: SolarWinds and SUNBURST Update

Author: Victor Sandin and Darby Wise

Executive Summary

On December 15, Infoblox released a Cyber Threat Advisory on the supply chain attack affecting SolarWinds' Orion IT monitoring and management software.[1] This advisory detailed FireEye's report on the campaign, including analysis on the SUNBURST backdoor, initial information on the threat actor's tactics, techniques and procedures (TTPs), as well as the mitigations and indicators of compromise (IOCs) that were most current at the time.[2] The threat actor behind the campaign carried out a complex attack chain and demonstrated highly sophisticated TTPs, indicating it was the work of an advanced persistent threat (APT) group. Known victims include government agencies, as well as private sector and critical infrastructure organizations.[3]

Since the publishing of our previous report, we have gathered additional information about the wide-ranging effects of this campaign, and are conducting several internal investigations. We are publishing this update to share some of the latest information from OSINT, as well as convey what we have been able to validate. This report also includes additional IOCs.

Analysis

Updates on Supply Chain Attack

As previously reported, the threat actor used a highly sophisticated attack chain to deliver malicious code via a backdoor injected into a dynamic-link library (DLL) that was a part of a legitimate update to some versions of SolarWinds Orion software (*SolarWinds.Orion.Core.BusinessLayer.dll*). Based on the update release date and passive DNS (pDNS) data, this breach started as early as March 2020. However, ReversingLabs has reportedly found that in October 2019, the threat actor distributed malicious files without the embedded backdoor to test whether or not these files would be detected.[4]

The threat actor was able to remain undetected for an extended period of time by employing sophisticated obfuscation methods such as imitating the legitimate SolarWinds coding style and naming standards, using virtual private servers (VPSs) with IPs native to the victim's home country, and leveraging compromised security tokens for lateral movement. Further analysis indicates that the threat actor used escalated Active Directory privileges to compromise the Security Assertion Markup Language (SAML) signing certificate and create valid tokens that could be used to access environment resources for data exfiltration.

According to a new alert from the Cybersecurity and Infrastructure Security Agency (CISA), it appears that the threat actor used multiple initial access vectors in addition to the SolarWinds Orion platforms. Volexity reported to have evidence connecting the TTPs from this campaign to multiple incidents from late 2019 and early 2020 targeting a US-based think tank. Volexity designated the actor responsible for these attacks Dark Halo.[5] In one of these incidents, Volexity observed the APT using a stolen secret key, known as an akey, to generate a cookie

to bypass the Duo multi-factor authentication (MFA) service and access a user's email via the Outlook Web App (OWA). While we are still investigating our non-Orion products, to date, we have not seen evidence that they are impacted by SUNBURST.

Our previous report included information from FireEye stating the APT deployed other variants of malware as additional payloads, including TEARDROP, SUPERNOVA, and COSIMICGALE. Since then, ZDNet has come out in agreement that the threat actor downloaded TEARDROP, a memory-only dropper, but also reported that security researchers' and Microsoft's further analysis indicates SUPERNOVA and COSMICGALE were not part of this campaign's attack chain and should be considered as a separate attack targeting CVE-2019-8917.[6]

Decoding the DGA Algorithm

Several teams have published findings pertaining to decoding the elements of the FQDNs created by the threat actor's DGA. The RedDrip Team from QiAnXin Technology published a decoder and that the structures of the subdomains were composed of three parts: a globally unique identifier (GUID) value composed of the hash of the hostname and MAC address of the first or default active and non-loopback interface; a single byte indicating if it is the first, second or third part of the payload (infected system domain name); and finally, a custom base32-encoded hostname to identify the victim. Longer domains are split across multiple queries and assembled later by matching the GUID section after applying a byte-by-byte exclusive OR.[7,8]

- The decoded value for the single byte indicating which part of the payload the subdomain includes ranges from 0 to 35. The first part of the payload will have a byte value of 0 if the domain is long enough to require multiple requests. Infected systems with short domain names will have only one request with a byte value of 35.

Subsequently, the NETRESEC team created a tool to further decode the SUNBURST subdomains in an effort to help identify SUNBURST victims. Since 18 December, they have released several versions of the decoder.[9]

DNS Activity

From a DNS perspective, Infoblox has been able to verify that once a victim has been infected with SUNBURST, the malware beacons to avsvmcloud[.]com with a hostname designed by a DGA to exfiltrate data about the victim, as described above. The threat actor can return one of several responses in the form of an IP. We have not yet been able to determine, nor seen reporting in OSINT, about what factor(s) trigger different responses from the threat actor. From our analysis it appears that the number of entities that receive direction to move to the second stage domains, passed via a CNAME resolution, is much smaller than the overall number that contact the initial server. It remains unclear how the actor chooses which victims to move into different stages of the attack.

Our analysis has also shown that if queries resolve to an IP that matches a pattern producing an address family as "NetBios," it appears to trigger certain follow-on activity. IPs match a pattern producing an address family as "Implink" or "Atm" serve as prompts for enumerating processes and services. IPs that resolve as "Ipx" appear to be requests for updates to local "Status" configurations. Infoblox has not observed data to confirm this. Other address families appear to include "InterNetwork," "InterNetworkV6," and "Error."

Prevention and Mitigation

FireEye, in coordination with GoDaddy, recently transferred control of the command and control (C&C) domain (avsvmcloud[.]com) to Microsoft to disable the SUNBURST backdoor from further execution.[10] GoDaddy created a wildcard DNS resolution ensuring any subdomain of the threat actor's C&C resolving to an IP address will not prompt any follow-on actions.

While this new DNS resolution will disable SUNBURST backdoor deployments connecting to the C&C, FireEye has stated that the attackers may have deployed other backdoors preventing the victims from removing the threat actor completely from their networks.

CISA included in their alert detailed mitigations for organizations that use the specific products affected by this attack chain.[3]

FireEye recommends the following upgrades to its affected customers, if possible:

- Customers using Orion Platform v2020.2 with no hotfix or 2020.2.1 HF1 should upgrade to 2020.2.1 HF 2, or
- Customers using Orion Platform v2019.4 HF 5 should upgrade to 2019.4 HF 6.

If an organization is unable to upgrade to this version of Orion, FireEye recommends taking the following actions:

- Disconnect SolarWinds servers from the Internet and isolate them, or restrict access from SolarWinds servers if this is not possible.
- Rotate credentials to accounts that have access to SolarWinds servers and/or infrastructure.
- Review network configurations created by SolarWinds, looking for anomalies.

Microsoft's Security Response Center has also provided important steps customers should take to protect themselves from the recent nation state activity.[11]

It is important to block all communications to the threat actor's C&C servers that are listed in the IOC table, as well as any further indicators released by security vendors confirmed to be part of this campaign.

Endnotes

1. https://blogs.infoblox.com/cyber-threat-intelligence/cyber-threat-advisory-solarwinds-supply-chain-attack/
2. https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
3. https://us-cert.cisa.gov/ncas/alerts/aa20-352a
4. https://blog.reversinglabs.com/blog/sunburst-the-next-level-of-stealth
5. https://www.volexity.com/blog/2020/12/14/dark-halo-leverages-solarwinds-compromise-to-breach-organizations/
6. https://www.zdnet.com/article/a-second-hacking-group-has-targeted-solarwinds-systems/
7. https://blog.cloudflare.com/a-quirk-in-the-sunburst-dga-algorithm/
8. https://blog.truesec.com/2020/12/17/the-solarwinds-orion-sunburst-supply-chain-attack/
9. https://www.netresec.com/?page=Blog&month=2020-12&post=Reassembling-Victim-Domain-Fragments-from-SUNBURST-DNS
10. https://krebsonsecurity.com/2020/12/malicious-domain-in-solarwinds-hack-turned-into-killswitch/
11. https://msrc-blog.microsoft.com/2020/12/13/customer-guidance-on-recent-nation-state-cyber-attacks/

Infoblox Cyber Intelligence Unit

With 10 years of experience, the Infoblox Cyber Intelligence Unit creates, aggregates and curates information on threats to provide actionable intelligence that is high-quality, timely and reliable. Threat information from Infoblox minimizes false positives, so you can be confident in what you are blocking, while ensuring a unified security policy across the entire security infrastructure.

Infoblox Threat Intelligence

Infoblox Threat Intelligence enables threat protection using timely and accurate data to minimize organizational risk and protect against cyberattacks. Our data is curated from more than two dozen partners, and our key sources include leading threat intelligence providers, government agencies, universities, as well as the Department of Homeland Security's Automated Indicator Sharing program. Infoblox Threat Intelligence provides a single platform for managing and distributing all of our licensed data sets within an organization's ecosystem.

Infoblox

Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud net-working today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70% of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com