Infoblox

The Infoblox Q1 2021

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 Q1 2021 report includes our publicly released threat intelligence from January 1, 2021, through March 31, 2021.

This publication provides our original research and insight into threats we observed leading up to and including this period of time. Our report includes a 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.

During Q1 2021, the Infoblox Cyber Intelligence Unit (CIU) has published reports on campaigns delivering:

- Valyria Trojan Drops Emotet
- Snake Keylogger
- Italian Emotet
- GhostDNS Exploit Kit
- Tax-Themed Phishing Campaign
- Buer Loader Trojan
- RuRAT Trojan
- BazarStrike
- Warezov Worm
- Dridex Banking Trojan
- Hancitor Downloader
- Trickbot Loader
- Burkina Trojan

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.

Cloud Vulnerabilities Remain Front and Center

The cloud transformation presents a learning curve that has been perhaps too steep for many. In several ways, even the most capable enterprise security architects have to start from scratch to determine what security controls were necessary to protect new cloud environments. In addition, many new vendors have to invent the security controls uniquely required by various cloud environments. Cloud architecture needed new security controls for which there is no exact analog in the on-premises world.

Most of these new security controls are not well integrated, if at all. Hybrid environments with both cloud and on-premises components make security much more difficult. One of the leading causes of cloud breach vulnerability continues to be errors in cloud administration, configuration and setup, including too many points of administration and different dashboards, as well as too many policies to propagate, synchronize and maintain consistently.

Most organizations will admit privately that they still don't have adequate cloud security deployment. To gain protection for the cloud, you might require a cloud access security broker (CASB), a cloud workload protection platform (CWPP) and cloud security posture management (CSPM) security controls. You will likely require integrations to many custom pieces of software and other security control program products. In addition, you will need to acquire and implement a security orchestration, automation and response (SOAR) platform, step up in a meaningful way to Zero Trust, and find your way forward with secure access service edge (SASE).

DNS security is also an important part of protecting your cloud resources. DNS security is one of the few technology sets that will protect on-premises, cloud and work from anywhere (WFA) users and resources from one central administration point. Architecture requirements for large enterprises and government remain almost completely committed to hybrid as they have both on-premises and cloud resources to protect. New controls to secure container-based workloads, lock down cloud configurations and encrypt data in the cloud are still being deployed.

As we noted last quarter, the security stacks that many organizations use don't scale easily if at all from on-premises to the cloud. Organizations would need a new version of data loss prevention (DLP) or digital rights management (DRM), in addition to other software and integrations for cloud environments. With new points of administration and management, plus a new front-end configuration, come opportunities for error and a potential data breach.

The SolarWinds Attack

On December 13, FireEye publicly disclosed information about a supply chain attack affecting SolarWinds' Orion IT monitoring and management software. The Infoblox CIU initially published our Cyberthreat Advisory on the same topic on December 15.

This cyberattack infected all versions of SolarWinds' 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.

In a January 5 joint statement, the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI) and the National Security Agency (NSA) indicated that based on their investigations, the APT is likely Russian in origin. Known victims include government agencies, as well as the private sector and critical infrastructure organizations.

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 that was a part of a legitimate update to some versions of SolarWinds' Orion software.

The threat actor was able to remain undetected for an extended 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.

From a Domain Name System (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 domain generation algorithm (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.

From our analysis to date, it appears that the number of entities receiving direction to move to the second stage domains, passed via a CNAME resolution, is much smaller than the overall number contacting 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" that serve as prompts for enumerating processes and services. IPs that resolve as "Ipx" appear to request updates to local "Status" configurations. Infoblox has not observed data to confirm this sequence. Other address families appear to include "InterNetwork," "InterNetworkV6" and "Error."

The CI/CD Pipeline Is Under Assault

Code signing uses certificate-based digital signatures to sign executables and scripts to confirm the software author, as well as guarantee that the code has not been altered or corrupted since being signed. The process employs the use of a cryptographic hash to validate authenticity and integrity.

This process is designed to impart trust. Users who download signed software can assume that it is coming from a legitimate source and not by some third-party attempting to appear legitimate. Code signing affirms that users know the organization is the official publisher of the code and that no other third party has modified it since being signed.

CISA's analysis of the attack on SolarWinds concluded that the threat actors added a malicious version of the binary *SolarWinds.Orion.Core.BusinessLayer.dll* into the SolarWinds software lifecycle. This version was then digitally signed by a legitimate SolarWinds code signing certificate. The malicious code became trusted once it was digitally signed, defeating the purpose of code signing: providing reassurance to users that the code an organization distributes can be trusted.

Worse yet, this malicious code became part of the regular code distribution from SolarWinds. The threat actors were able to widely propagate this malicious module to SolarWinds customers and subsequently call out to external domains using a protocol that copied legitimate SolarWinds protocol traffic. Once the command and control (C&C) was set up, the threat actors continued their attack.

Crafting a strategy to breach a software provider's most secured continuous integration/continuous delivery (CI/CD) pipeline means threat actors are aiming for the heart of cyberdefenses. By successfully breaching the CI/CD pipeline, threat actors would assume a mantle of trust and are capable, virtually unhindered, of using an organization's trusted reputation to distribute malware across its user base, potentially enabling serious and widespread damage.

The problem is not with the code signing, but rather the fact that once highly sophisticated threat actors are deep inside and undetected within a supplier's networks, they can find opportunities to break what ordinarily would be a highly secure process. They can observe a software supplier's day-to-day operations and find opportunities to insert themselves and their malicious code into these process flows. Given this new challenge, software suppliers need to review their code signing policies and strategies for private key storage, improve control of their process flow and consider how to manage their inventory of code signing certificates more closely.

Work from Anywhere Environments

With many organizations allowing users to utilize home broadband connections for work use, the corporate attack surface has grown substantially, with sensitive data being strewn and exposed everywhere. None of this has changed in Q1 2021.

According to the "Enduring From Home" report based on the Malwarebytes survey of 200 companies:[1]

- 70 percent of the companies moved 61 percent or more of their workforce to a WFA environment
- 43 percent of the companies with 100–700 employees moved 61–80 percent of their workforce home
- 38 percent of companies with 700 or more employees moved 81–100 percent of their employees home

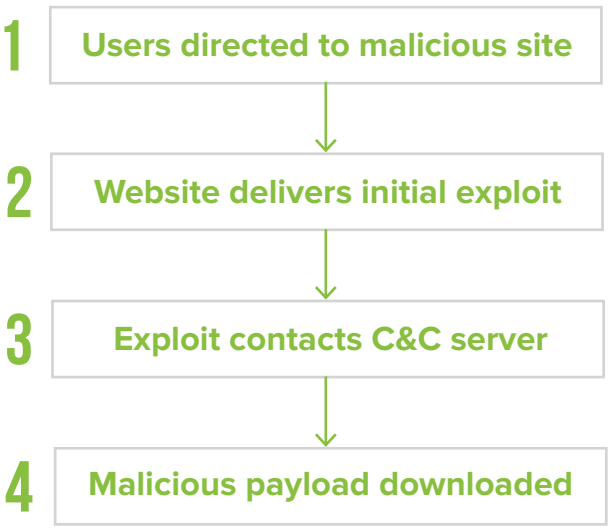
Organizations have continued to implement strategies to protect users and network-connected resources in WFA environments. Even as the pandemic will ultimately ease in the future, WFA environments will still remain as a viable alternative and continue to be used by most organizations.

As part of the challenge, WFA brings many pitfalls that have not yet been remediated. The proliferation of untrusted home networks, often containing many varieties of malware, and untrusted home devices, most without properly configured firewalls or endpoint security, has opened up many more risks for devices that access corporate networks.

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. Remote workers require access to enterprise resources from multiple endpoints, including both employer-provided and personal laptops, plus a variety of mobile devices. WFA access must be granted not only to employees but also to business partners because these partners require access to resources both on-premises and in the cloud.

However, many cybersecurity procedures and security controls used within enterprise facilities cannot provide adequate security for the locations that WFA employees use. The on-premises legacy enterprise security stack will not work for remote workers without significant redesign and the addition of new security controls to support distributed infrastructure and cloud deployments.

1. https://resources.malwarebytes.com/files/2020/08/Malwarebytes_EnduringFromHome_Report_FINAL.pdf



DNS is used for all external destination lookups

FIgure 1: Work from Anywhere (WFA) Techniques of Choice

Note that DNS security can be configured to substantially protect WFA workers. Many organizations do not yet have the additional protections and visibility that DNS security deployment would provide. Often, one of the earliest steps in the execution of a threat actor's attack chain is the use of DNS to reach out to malicious domains and establish C&C communications. With DNS security, an organization can deploy one technology set, with a consistent administrative and management interface, to protect all of its on-premises, cloud and WFA activity.

The same is true for expanded threat intelligence data, which can provide a strategic advantage to an organization's cyberdefenses by focusing increased security on areas that threat actors frequently use.

The Most Common Types of Cyberattacks

Email Remains the Leading Attack Vector

Email remains the top threat vector used to attack both government and businesses of all sizes. Email delivers 75 to over 90 percent of malware. Despite training and widespread warnings against malspam, users continue to open suspicious emails, both in their business and personal accounts. They click on malicious email attachments and URLs, as well as view websites not generally associated with business use.

The Infoblox CIU continues to observe widespread threat actor use of email campaigns employing social engineering tactics to propagate a variety of attacks. In some instances, these attacks are highly targeted to one individual or organization, a technique known as spear-phishing, but larger campaigns are more common.

Phishing emails seek users' engagement to spread malware into their system and, potentially, an organization's business network. Threat actors target consumers and business users with email or text messages to lure them into revealing confidential information such as passwords, account numbers or Social Security numbers. Once they steal this information, they can then gain access to email, bank or other accounts. Threat actors continue to launch thousands of phishing attacks daily.

Phishing emails often appear as though they are from a recognizable company with a well-known brand. These may include financial institutions, social network sites or online stores. They often use social engineering techniques that help to lure users into clicking on an attachment or a potentially malicious link, allowing the malware to spread and the cyberattacker to access the user's system.

Anatomy of a Phishing Attack

The phishing attack against the California State Controller's Office (SCO) this past month (March 2021) is a recent example. The SCO manages over $100 billion of public financial assets annually. This attack is the tip of an iceberg representing the many phishing campaigns threat actors launch each month worldwide.

Per the SCO, an employee of the SCO Unclaimed Property Division clicked on a link in an email that appeared to come from a trusted outside entity. Clicking on this link unknowingly provided an unauthorized user with access to the employee's email account. The unauthorized user had access to the account from March 18, 2021, at 1:42 p.m. to March 19, 2021, at 3:19 p.m. and sent potentially malicious emails to some of the SCO employee's contacts.

Remediation by the SCO was fast but not enough to mitigate all of the impact. The SCO has reason to believe the compromised email account had personal identifiable information (PII) contained in Unclaimed Property Holder Reports.

Unfortunately, that PII potentially includes property owners' first and last names, addresses, Social Security numbers, birth dates and the values of the items turned over to the SCO. The loss of this kind of PII can be a dangerous breach. PII represents some of the most valuable information to threat actors. Once they have this information, the potential for additional damage and fraud is high.

The SCO promptly discovered the improperly accessed email account and removed access to it. Personnel of the SCO Unclaimed Property Division immediately began a review of all emails in the account for PII that may have been viewed. They also advised all contacts of the SCO employee to delete suspicious emails and avoid clicking on any links they encounter.

The SCO also advised individuals and companies to place a fraud alert on their credit files and suggested privacy protection steps that included contacting the three major credit bureaus to report the potential identity theft. All of this was the result of one single successful phishing email.

Ransomware as a Service

The widespread use of ransomware continues unabated into Q1 2021, with ransomware tools increasing in sophistication. Ransomware-as-a-service (RaaS) platforms can be easily deployed by even the least technical ransomware threat actor. As threat actors become more skilled and capable at using ransomware, they are executing increasingly more damaging attacks, often against enterprises and government organizations.

Threat actors are also becoming more selective and will target specific organizations with carefully researched social engineering tactics. Well-crafted email is used to entice targets to click on dangerous URLs or open malicious attachments. Most attacks would be unsuccessful without user engagement.

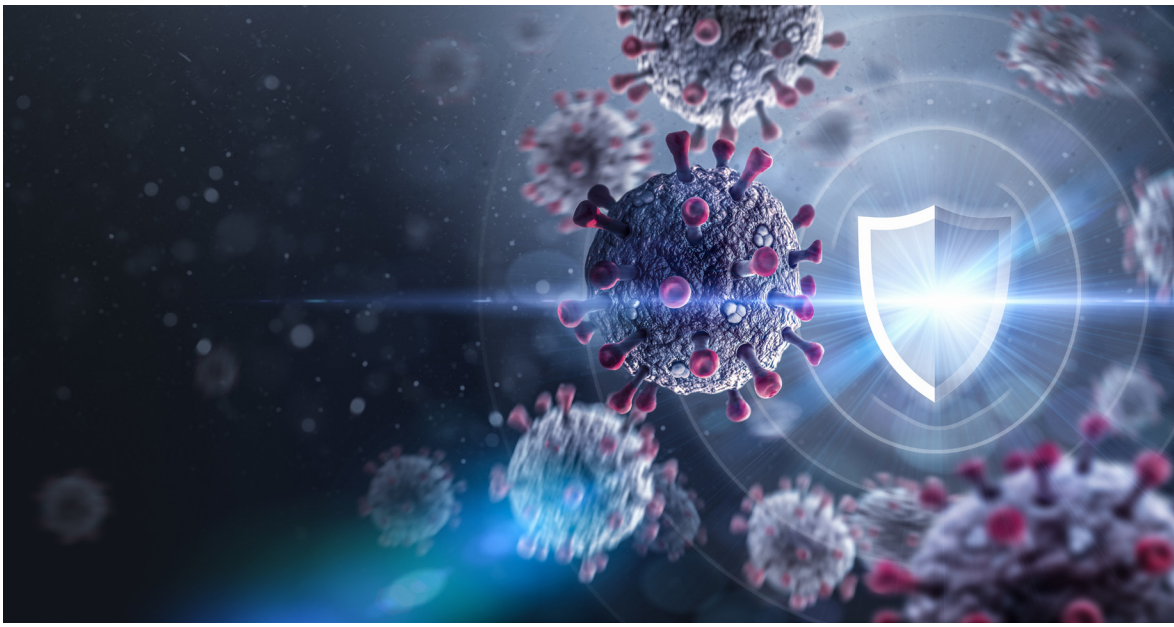
As before, the effects of successful ransomware attacks can be crippling. In some circumstances, the road to recovery for organizations impacted is very unclear.

COVID-19 Remains a Top Theme for Social Engineering

COVID-19 has continued to present threat actors with new opportunities. Over the past year, there has been an endless progression of COVID-related phishing attacks. As these attacks ramped up through 2020, Google alone blocked a reported average of 18 million daily malicious COVID-19 messages to Gmail users. Beyond malware and phishing email, Google also blocked more than 240 million spam messages related to COVID-19.[2]

2020 saw threat actors successfully impersonating government authorities such as the World Health Organization (WHO). You can see our report on Trickbot WHO?, which used a fraudulent coronavirus alert from the WHO to deliver Trickbot banking malware. Other emails impersonated UNICEF and attempted to leverage psychological manipulation by posing as a children's charity. You can see our earlier reports on coronavirus-related themes to get a sense of the depth and breadth of these campaigns. Earlier reports include COVID-19 Unemployment Fraud, Formbook Coronavirus Campaigns, New Agent Tesler Infostealer Campaigns Use Coronavirus Themes, Spoofed Coronavirus Map Delivers AZORult Infostealer and LokiBot Rides Fear of Coronavirus.

Looking at it through its impact on the financial community, COVID-19, overall, is credited for a 238 percent rise[3] in cyberattacks targeted against banks throughout 2020.



2. https://www.businessinsider.com/google-says-gmail-blocked-18-million-coronavirus-phishing-emails-2020-4

3. https://www.zdnet.com/article/covid-19-blamed-for-238-surge-in-cyberattacks-against-banks/

Tracking Cybersecurity and Data Privacy Regulation

Compliance requirements also generate large demands on organizations with respect to data privacy and cybersecurity. This rising tide of data privacy and cybersecurity regulation continues to grow at the municipal, state and federal level both in the United States and worldwide.

Several bills are moving through the U.S. House of Representatives and the Senate to specifically address cybersecurity funding, preparation, response, resiliency and recovery related to cyberthreats and incidents impacting state and local government.

These include:

- S.1065 State Cyber Resiliency Act
- S.1846 State and Local Government Cybersecurity Act of 2019
- H.R.5823 State and Local Cybersecurity Improvement Act

Late last year, California voters passed the California Privacy Rights Act (CPRA), which impacts the California Consumer Privacy Act (CCPA), a law to enhance privacy rights and consumer protection for residents of California. This new legislation will create a new agency, the California Privacy Protection Agency, which will begin enforcement by or before 2022. This agency will have full administrative power, authority and jurisdiction to implement and enforce the CCPA and the CPRA.

In Washington State, the Washington Privacy Act (WPA) legislation is in process and would take effect July 2022 if it passes. The WPA seems to contain the spirit and intent of provisions in the CCPA and in some cases, the European Union's General Data Protection Regulation.

There are many other bills moving forward in Connecticut, Oklahoma, Virginia, New York, Mississippi and Minnesota. There are also specific laws coming in Maryland and New York that address the data privacy of biometric data, as well as considerable activity in this area in Illinois with the Illinois Biometric Information Privacy Act (BIPA).

In our Q4 2020 Cyberthreat Intelligence Report, we noted that 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 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 benefit from it as they purchase devices designed in compliance with the act.

In regard to interest in IoT legislation, note that NIST was to publish standards and guidelines on March 4, 2021, but it needs to gather more data from the public domain before finalizing the standards. On June 3, the IoT Act requires that NIST, with the support of the Department of Homeland Security and the Office of Management and Budget, publish guidelines on the management of IoT security vulnerabilities that are relevant to government information systems. And in December 2022, the IoT Act will halt the acquisition by any federal agency of IoT devices if the agency's chief information security officer determines that these IoT devices are not compliant with the NIST standards.

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.

January 2021

Threat Reports & Cyberthreat Alerts

Valyria Trojan Drops Emotet

During the week of January 4, we observed a malspam campaign distributing the Valyria trojan. The emails in this campaign contain an error message when opened and execute a PowerShell script via Windows Management Instrumentation.

Read the Full Report ➜

Snake Keylogger Slithers Through Malspam

During the week of January 14, we observed a malspam campaign distributing the Snake Keylogger. The emails in the campaign contain a malicious 7-ZIP archive that opens an SCR file and downloads the malware to the victim host.

Read the Full Report ➜

Italian Emotet Campaign

On January 22, Infoblox observed a large malspam campaign targeting Italian speakers and delivering Emotet malware. This campaign delivered emails containing malicious, password-protected ZIP archives with a Microsoft Word document that infects victims when opened. We have also reported on previous Emotet campaigns, which we reference in this latest report.

Read the Full Report ➜

GhostDNS Exploit Kit

On January 26, Team Cymru posted an update to their analysis of the GhostDNS exploit kit. Their report detailed an ongoing GhostDNS campaign that targets unsuspecting users by compromising and changing the DNS of their router to deliver phishing websites.

Read the Full Report ➜

Cyber Threat Advisory - SolarWinds Second Update

On December 15, Infoblox released a Cyber Threat Advisory on the supply chain attack affecting SolarWinds' Orion IT monitoring and management software. 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.

January's update includes new information provided by the latest alert from CISA and recent OSINT on additional attack vectors, use of anti-analysis blocklists, additional information in privilege escalation and persistence, compromised accounts and applications in Azure/ Microsoft 365 environments, and command and control protocol. We have also updated the IOC table with new information.

Read the Full Alert ➜

February 2021

Threat Reports & Cyberthreat Alerts

Tax-Themed Phishing Campaign

On February 1, we observed a malspam campaign distributing a Hypertext Markup Language (HTML) file designed to steal email credentials from the recipient. The campaign's email subject references tax documents. In the United States, it is not unusual to see campaigns using tax-related lures at this time of the year.

Read the Full Report ➜

Buer Loader Campaign Spoofs Identity Services Company

From February 2 to 10, Infoblox observed an ongoing malspam campaign delivering trojan malware known as Buer Loader. This campaign used invoice-themed lures to entice users to download and open Microsoft Excel (XLS) documents that contain malicious macros and spoof GlobalSign, a legitimate identity services company.

Read the Full Report ➜

Malspam Campaign with Fake Invoice Drops RuRAT

On February 15, Infoblox observed a malicious email campaign distributing a remote access trojan (RAT) known as RuRAT, via an encrypted XLS spreadsheet with malicious macros. In this campaign, threat actor(s) used an email subject referencing a fraudulent card invoice to lure users into opening the malicious attachment for details.

Read the Full Report ➜

BazarStrike Malspam Campaign Spoofs Complaint Notifications

During the week of February 22, security researchers discovered email campaigns distributing a malware loader for Cobalt Strike, a legitimate penetration testing tool abused by threat actors for its post-exploitation capabilities. These campaigns, which some researchers have nicknamed "BazarStrike," deliver the loaders using similar tactics, techniques and procedures to those of BazarLoader campaigns.

Read the Full Report ➜

Cyber Threat Advisory - HIDDEN COBRA: AppleJeus Cryptocurrency Threats

On February 17, the Cybersecurity Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Treasury (Treasury) published a joint report to highlight the cyber threat posed to cryptocurrency by North Korea, formally known as the Democratic People's Republic of Korea (DPRK); the report also provides mitigation recommendations and indicators of compromise for detection. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA.

Read the Full Alert ➜

Cyber Threat Advisory - TEARDROP Malware

On February 8, the Cybersecurity and Infrastructure Security Agency (CISA) published a Malware Analysis Report (MAR) on malware related to the supply chain attack on SolarWinds' Orion platform that was discovered in December 2020. Cybersecurity company FireEye has named this malware TEARDROP. The report details the analysis of a trojan backdoor that decrypts and executes an embedded payload – Cobalt Strike Beacon Implant (Version 4) – that enables the attacker to remotely control infected systems through an encrypted network tunnel.

Read the Full Alert ➜

Cyber Threat Advisory - SUPERNOVA Malware

On January 27, the Cybersecurity & Infrastructure Security Agency (CISA) published a Malware Analysis Report (MAR) on malware affecting SolarWinds' Orion platform. Cybersecurity company FireEye has named the malware SUPERNOVA. Both CISA and SolarWinds assessed that SUPERNOVA is not related to the supply chain attack on SolarWinds that was discovered in December 2020 but was designed to appear as part of the SolarWinds product. The report details the analysis of a PowerShell script that installs a malicious webshell backdoor – SUPERNOVA – allowing an attacker to inject and execute C# code into the SolarWinds software.

Read the Full Alert ➜

March 2021

Threat Reports & Cyberthreat Alerts

Warezov Worm Malspam Campaign

From March 1 to 3, we observed a malspam campaign distributing the Warezov worm. Also known as Stration, Warezov is an email worm first seen in 2006; it is spread through executable (EXE) files sent via email. This malware was most prevalent between 2006 and 2008, with little public reporting on it since then. It is known for frequently downloading new variants of its code from remote servers. Infoblox last reported on a major Warezov campaign in 2019. In this most recent campaign, both the body of the emails and the file names have changed, but the subject line as well as the C&C server remain the same as in the 2019 campaign.

Read the Full Report ➜

Malspam Campaign Spoofing Shipping Company Quote Drops Dridex Banking Trojan

On March 12, Infoblox observed a malspam email campaign distributing the Dridex banking trojan via emails spoofing updated/adjusted invoice notifications from the shipping company Freight Quote. Previous Infoblox reporting has highlighted Dridex campaigns distributing malspam masquerading as legitimate emails from organizations such as Intuit and Automatic Data Processing, Inc.

Read the Full Report ➜

Hancitor Downloader Delivers Cobalt Strike and Ficker Stealer

On March 18, security researcher Brad Duncan reported a malspam campaign that 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. These copies of Hancitor delivered additional payloads containing Cobalt Strike and Ficker Stealer.

Read the Full Report ➜

Malicious Activity Report: Trickbot Loader

Recent activity from a Trickbot campaign targeting the insurance and legal sectors show that the botnet is still a threat, despite U.S. Cyber Command's attempt to disrupt it in October 2020. Given the potential impact of this threat, we are releasing this detailed report on Trickbot's functionality to provide our customers and security researchers with the knowledge to prepare for and defend against potential Trickbot-related threats. In this report, we describe Trickbot's packer and process execution chain, supply insight on identifiers generated by the malware, as well as detail its signature verification and persistence techniques. We include an explanation of the configuration and how it is decrypted during execution, along with an overview of the network flow and the capabilities of the C&C protocol.

Read the Full Report ➜

Malspam Campaign Delivers Burkina Trojan

From March 21 to 23, we observed a malspam campaign distributing the Burkina trojan. First seen in October 2017, Burkina is a trojan distributed through EXE files sent via email. Burkina infects a victim's computer and attempts to harvest credentials, interrupt standard processes, conceal network connections and take other malicious actions. The malware then reaches out to a C&C server to receive additional instructions.

Read the Full Report ➜

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 | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054
+1.408.986.4000 | info@infoblox.com | www.infoblox.com