

Q2 | 2021

CYBER THREAT REPORT



Powered by the
Infoblox Cyber Intelligence Unit

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	4
A Close Look at Ransomware	5
Ransomware Attack on JBS USA	6
Ransomware Attack on Colonial Pipeline	7
REvil Ransomware Attack on Kaseya	8
Ransomware as a Service (RaaS)	9
Ransomware as a Service Process Flow	10
Ransomware Distribution Methods.....	11
NIST’s Cybersecurity Framework Profile for Ransomware Risk Management	14
CISA’s New Ransomware Readiness Assessment	14
Ransomware Mitigations.....	15
CISA and FBI Discourage Paying Ransoms.....	16
Insurers Might Drop Ransomware Coverage	16
The Federal Government Steps up on Cybersecurity	17
NSA’s and CISA’s Guidance on DNS Security	19
Tracking Cybersecurity and Data Privacy Regulation	20
Security Breach Notification Laws	22
Q2 2021 Cyber Campaign Briefs and Cyberthreat Alerts	23
The Infoblox Cyber Intelligence Unit	27
Infoblox Threat Intelligence	27



Executive Summary


We at Infoblox are pleased to publish this edition of our Quarterly Cyberthreat Intelligence Report. We publish these reports during the first month of each calendar quarter.

This publication supplements 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 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 protecting the community at large.

Usually, we report on specific threats and related data, customer impacts, analysis of campaign execution and attack chains, as well as vulnerabilities and mitigation steps. We also share background information on the attack groups likely responsible for the particular threats under review.

During Q2 2021, the Infoblox Cyber Intelligence Unit (CIU) published reports on campaigns that delivered the following:

- ➔ [Malspam Campaign Spoofing Waybill Delivers Nanocore Rat \(June 28, 2021\)](#)
- ➔ [Hancitor Downloads Infostealers \(June 22, 2021\)](#)
- ➔ [Shathak Pushes IcedID Banking Trojan \(June 9, 2021\)](#)
- ➔ [RemcosRAT Malspam Campaign Spoofs UAE Machinery Company Correspondence \(June 2, 2021\)](#)
- ➔ [Cyberthreat Advisory - Nobelium Campaigns and Malware \(June 2, 2021\)](#)
- ➔ [Graftor Adware Still Circulating \(May 27, 2021\)](#)
- ➔ [Biotech-Themed Malspam Drops BitRAT \(May 18, 2021\)](#)
- ➔ [Cyberthreat Advisory: DarkSide Ransomware Attack on Colonial Pipeline \(May 13, 2021\)](#)
- ➔ [Malspam Delivering Agent Tesla Keylogger Spoofs Oil & Gas Co. Messages \(May 12, 2021\)](#)
- ➔ [Cyberthreat Advisory: FiveHands Ransomware \(May 10, 2021\)](#)
- ➔ [Polish Language Malspam Campaign Delivers AveMaria Infostealer \(May 3, 2021\)](#)
- ➔ [Post-Takedown Trickbot Activity \(April 28, 2021\)](#)
- ➔ [Spoofed Vehicle Purchase Invoice Malspam Drops Formbook Infostealer \(April 16, 2021\)](#)
- ➔ [Agent Tesla Malspam Campaign Spoofs Bank Correspondence \(April 13, 2021\)](#)
- ➔ [Italian Economic Support-Themed Malspam Delivers Ursnif Banking Trojan \(April 1, 2021\)](#)



Most recently, 35 percent of businesses that have paid ransoms provided between \$350,000 and \$1.4 million, and 7 percent of businesses paid ransoms in excess of \$1.4 million.¹

A Close Look at Ransomware

Ransomware is once again front and center in our quarterly threat report. This year has turned out to be one of the worst years for ransomware. Why? Because that's where the big money is. Large potential return on investment makes ransomware extortion activities highly compelling for threat actors.

Ransomware allows for big payoffs with a minimal chance of getting physically caught. The ransomware threat actors are often thousands of miles away from their targets, there is little to no interference from law enforcement agencies, and extradition for ransomware crimes is rare or non-existent. Threat actors have everything to gain and almost nothing to lose beyond their investment in cyber offense tools and the time they spend on the attack.

On June 16, Cybereason released a study that surveyed approximately 1,300 security professionals.¹ The study reveals that more than half of organizations surveyed have fallen victim to ransomware attacks. In addition, 80 percent of businesses that have paid ransoms have suffered second ransomware attacks, often from the same threat actors.

The impact and expense of successful ransomware attacks can be crippling to an organization. In 2020, payments associated with ransomware² have been estimated at \$370 million. However, ransomware costs are not just about the ransom payouts; the total damage associated with ransomware is estimated to be much higher than the payouts—perhaps \$20 billion.³

Verizon's 2021 Data Breach Investigations Report⁴ notes, "The novel fact is that 10 percent of all breaches now involve ransomware."

Ransomware-related damages continue to increase. They include the loss of data, damage to or destruction of information systems and operational infrastructure, losses to productivity, and damage to brand and reputation. The Cybereason study also showed that 66 percent of surveyed organizations reported significant loss of revenue after a ransomware attack, 53 percent of indicated that their brand and reputation were damaged as a result of a successful attack, and 32 percent reported losing C-level talent as a direct result of ransomware attacks. As many as 26 percent of organizations reported that ransomware attacks forced their businesses to close temporarily.⁵

1. <https://www.cybereason.com/press/new-cybereason-ransomware-study-reveals-true-cost-to-business>
2. <https://www.cnb.com/2021/04/06/the-extortion-economy-inside-the-shadowy-world-of-ransomware-payouts.html>
3. <https://purplesec.us/resources/cyber-security-statistics/ransomware/>
4. <https://enterprise.verizon.com/resources/reports/2021-data-breach-investigations-report.pdf>
5. <https://www.cybereason.com/press/new-cybereason-ransomware-study-reveals-true-cost-to-business>

Ransomware Attack on JBS USA

JBS USA was very recently the victim of a massive and well-publicized ransomware attack. JBS USA is part of [JBS Foods](#), one of the largest food distributors in the world. The company has operations in 15 countries and customers in almost 100 countries. Its [brands](#) include Pilgrim's, Great Southern and Aberdeen Black.

JBS spends over \$200 million on IT annually and has more than 850 information technology employees worldwide. JBS has very capable IT, security operations and network operations.

In May, JBS paid an \$11 million ransom after a cyberattack shut down the company's entire beef processing operation in the U.S. The attack apparently targeted and disrupted JBS servers in North America and Australia. Production was disrupted for several days, and JBS took precautions to carefully check the IT resources within its networks before bringing them back online.

Currently, the Federal Bureau of Investigation (FBI) believes the ransomware attack was perpetrated by the threat actor [REvil](#): a group believed to be based in Russia or eastern Europe. REvil has made its malware available as a ransomware-as-a-service (RaaS) and has successfully taken money from many organizations since 2020.

The ransomware attack on JBS resulted in the temporary curtailment of operations and affected approximately one-fifth of the U.S. meat supply. The attack's broad impact led to concerns about a shortage of beef and pork and about a possible increase in the prices of these commodities.





Ransomware Attack on Colonial Pipeline

Colonial Pipeline was another victim of a recent high-profile attack. In early May, the threat actors behind DarkSide⁶ ransomware gained access to the company's IT infrastructure. The company moved quickly and shut down 5,550 miles of its pipeline.

Colonial Pipeline is a company responsible for producing almost half of all fuel consumed on the East Coast of the United States.

To fully restore its systems, the company had to pay the ransom of 75 bitcoin—at that time, roughly \$4.4 million. Also, the shutdown left fuel stranded on the Gulf Coast; this caused a shortage of gasoline, panic buying, and a spike in prices.

DarkSide uses a RaaS malware sold to and deployed by affiliate organizations. The DarkSide group has a history of targeting organizations that are more likely to pay ransoms. By both encrypting and exfiltrating victims' data, the attackers gain double leverage: they not only freeze the company's data but also threaten to release it on a public-facing website.

Shortly after the attack on Colonial Pipeline, the Cybersecurity and Infrastructure Security Agency (CISA) advised owners and operators of operational technology (OT) assets and industrial control systems (ICS) about the extreme and mounting threat of ransomware. The [CISA advisory](#) provides a summary of the steps necessary to improve defenses in the face of mounting ransomware attacks.

Covert Effort Recovers Big Portion of Bitcoin Ransom Payment

DarkSide has not emerged unscathed from its attack on Colonial Pipeline. U.S. law enforcement landed a strong counterpunch and [recovered \\$2.3 million](#) in bitcoin paid in the Colonial Pipeline ransom. U.S. officials identified a virtual currency wallet that DarkSide threat actors used to collect the payment from Colonial Pipeline.² The activities associated with the seizure of the cryptocurrency ransom paid to the threat actors is the first publicly revealed instance of such action by any U.S. government agency. Thus far, the security and confidentiality of cryptocurrency has been a key enabler for ransomware actors.

Possible Involvement of FBI

The FBI has sometimes been able to access and obtain the encryption keys used by the attackers. This access enables the FBI to unlock the seized data without requiring the ransom payment. In the case of Colonial Pipeline, however, the FBI did not explain how it obtained a key for the specific bitcoin address. In the same case, the Justice Department did not provide any insight into the techniques and procedures that made the seizure possible, nor did it disclose any details on whether other government agencies were involved. However, it did note that law enforcement was able to monitor multiple transfers of the cryptocurrency.

6. <https://us-cert.cisa.gov/ncas/alerts/aa21-131a>

At a recent news conference on the seizure, Deputy Attorney General Lisa Monaco said, “By going after the entire ecosystem that fuels ransomware and digital extortion attacks, including criminal proceeds in the form of digital currency, we will continue to use all of our resources to increase the cost and consequences of ransomware and other cyber-based attacks.”

Security Directive

In the wake of the Colonial Pipeline ransomware attack, the Department of Homeland Security’s Transportation Security Administration announced a Security Directive that “will enable the Department to better identify, protect against, and respond to threats to critical companies in the pipeline sector.” The Security Directive⁷ will require pipeline owners and operators designated critical to report any suspected or confirmed cybersecurity incidents to the CISA. It will also require these owners and operators to review their current practices, perform a cybersecurity risk analysis to identify gaps and necessary remediation, and report the results within 30 days. Pipeline companies have been operating under voluntary guidelines, like many industries, and now might face fines if they fail to comply with security directives on required cybersecurity practices.

REvil Ransomware Attack on Kaseya

This is a late-breaking addition to our Q2 2021 report. On July 2, the threat actors behind REvil, a ransomware also known as Sodinokibi, launched a massive attack targeting users of Kaseya’s remote monitoring and management service, VSA. In this supply chain attack, the actors exploited a zero-day vulnerability in Kaseya’s software to deploy ransomware on nearly 1,500 company networks. Kaseya stated that the attack compromised only customers of the on-premises version of VSA and that there is no evidence that it compromised SaaS customers.

After the attack, the actors stated the following on their blog: “On Friday (02.07.2021) we launched an attack on MSP providers. More than a million systems were infected. If anyone wants to negotiate about universal decryptor – our price is 70,000,000\$ in BTC and we will publish publicly decryptor that decrypts files of all victims, so everyone will be able to recover from the attack in less than an hour.”

In June 2019, we published a report on Sodinokibi/REvil. At the time, it was a relatively new RaaS, and it appeared to be one of the ransomware families filling a void left by the discontinuation of the popular ransomware GandCrab. REvil was first identified in the wild on April 17, 2019, when threat actors exploited a vulnerability in Oracle WebLogic to install Sodinokibi on susceptible web servers. Like GandCrab, REvil uses an affiliate revenue system where threat actors sign up as affiliates, start using the ransomware for no initial fee, and share a percentage of their profits.

7. <https://www.dhs.gov/news/2021/05/27/dhs-announces-new-cybersecurity-requirements-critical-pipeline-owners-and-operators>

Threatening to expose a victim's data on a data-leak site, in addition to encrypting the victim's files, increases the leverage of a ransomware threat actor and is another part of the actor's strategy. Such exposure might be more damaging than the financial impact the victim would experience by paying a ransom.

As we noted in 2019, the fact that REvil is freely available means its distribution methods vary from one threat actor to another. Even in 2019, REvil affiliates had distributed the ransomware by compromising MSPs, sending out malicious spam emails, and hacking websites that host downloadable executables. To learn more about this latest ransomware attack on Kaseya, please refer to our cyber threat advisory [Kaseya REvil Ransomware Attack Cyber Threat Analysis](#) and our update [Kaseya Ransomware Attack Update: Patch Available](#).

Ransomware as a Service (RaaS)

The ransomware attacks on JBS and Colonial Pipeline are examples of criminal organizations using RaaS platforms. Many potential threat actors lacking the skills to build their own ransomware and to launch an attack with it can buy what they need through the dark web.

Nearly two-thirds of ransomware attacks during 2020 came from RaaS-based platforms.⁸

RaaS platforms include support, community forums, documentation, updates and more. They are closely modeled after the type of support offered with legitimate SaaS products. Some RaaS websites offer supporting marketing literature and user testimonials. The cost is relatively low. In some cases, affiliates can sign up for a one-time fee or for a monthly subscription. Some RaaS platforms are set up without any initial fees and share the fees associated with a successful attack. Other platforms might have charges for special features, such as the view of a status update of active ransom infections, the number of files encrypted, and payment information.

The use of highly targeted RaaS attacks has been lucrative for threat actors. Actors that use RaaS to target large organizations can, in turn, ask for large ransoms. In these highly targeted cases, threat actors sometimes use carefully researched social-engineering tactics, such as well-crafted emails, to entice targets to click dangerous URLs or open malicious attachments. In other cases, threat actors may target a vulnerability that is particular to or commonly used by their target victim group.

Several years ago, the Department of Health and Human Services Office of the Comptroller of the Currency (HHS OCR) created a requirement: For every ransomware attack that might have impacted more than 500 patient records, the attacked organization had to promptly report this to the HHS OCR as an assumed data breach. HHS treats ransomware attacks as data breaches because in order to encrypt a victim's data, the threat attacker must have access to it, which itself constitutes a data breach.⁹

8. <https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/>

9. <http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf>

Ransomware as a Service Process Flow

A ransomware attack can start with one of several distribution methods. In an email phishing attack, a seemingly legitimate email contains malicious attachments or links that initiate the download of ransomware.


Many types of ransomware can move through the target organization's networks, where antivirus software, firewalls, and endpoint security might be disabled or substantially compromised. Once this is accomplished, additional malicious tools might be downloaded, such as a backdoor that would enable remote access for the threat actor. Today, breached data files can be exfiltrated to locations specified by the threat actors, to support potential public disclosure of the data.

To communicate the ransom note, a splash screen opens or a TXT file is loaded to the desktop of the target's computer. The initial ransom communication is designed to make the victim pay the ransom quickly and to eliminate the possibility that law enforcement could intercede. To make the ransom payment, a victim may be directed to download a specific browser enabled for the dark web and to access a payment gateway where a cryptocurrency can be used.

In situations where ransom payments are laundered, the funds are transferred into and out of several cryptocurrency accounts and then to traditional bank accounts located in countries where law enforcement cannot obtain information on the accounts or related activities. After this laundering, the cryptocurrency might be converted to cash in a country outside of the reach of authorities in the victim's country.

For sophisticated threat actors and operations, the cash can be moved to businesses that are used as fronts and where the cash can be declared as legitimate and made available for use.

By converting the cryptocurrency ransom payment into cash, the threat actor hopes to break the electronic money-trail and thus thwart law enforcement's attempts to attribute the criminal activity to the actor.

A hand is shown interacting with a digital interface. The interface features a glowing blue line graph with several data points highlighted by small circles. Below the graph, there are various data elements, including a circular gauge showing '25%' and several rectangular boxes containing numbers like '3,7782', '2,3374', and '1,732'. The background is dark with a grid pattern, and the overall aesthetic is futuristic and technical.

Ransomware Distribution Methods

It is important to examine the distribution methods commonly used for malware, which can include ransomware, and then consider the mitigations necessary to eliminate or minimize successful use of these methods. While not exhaustive, the four distribution methods covered here are malicious websites, malspam email, remote desktop protocol, and USB memory sticks. Depending on the report cited, time period, and companies surveyed, the percentages of ransomware attacks that use these distribution methods have varied significantly.

Malicious Websites

A malicious website distributes harmful downloads to users socially engineered to click links to that site. In addition to setting up their own spoofed site, threat actors can find and exploit vulnerabilities in a legitimate website and implant malicious code on it. Alternatively, they may use it to redirect the target to another website under their control. Some of the most well-known media and sports websites in the world have at some point been compromised or hijacked.

Some malicious websites host exploit kits, which allow the threat actors to scan the target's endpoint for vulnerabilities. After finding vulnerabilities, the actors can execute code without the users clicking anything. The users will not realize their machines are infected until a ransom note appears and requests a payment in return for the decryption key or files.

Malvertising is also a closely related delivery mechanism for deploying malware, in which fake advertisements are placed on selected websites. In some cases, threat actors have purchased ads embedded with malware and have paid ad networks to deploy those ads.

A well-known example of this was the malvertising embedded in the *New York Times*¹⁰ Magazine in 2009. The online *New York Times Magazine* was serving ads from a network of infected computers that were part of the Bahama botnet. The banner feed of the *New York Times* was breached and manipulated during September 11 to 14. This caused some readers to see malvertisements telling them their systems were infected and manipulating them into clicking and installing rogue security software. Rogue security software tells a victim that they are infected and requests that the victim take action by clicking on something, which in fact, installs and propagates the malicious code.

Malspam Email

Threat actors consistently use email campaigns employing social engineering tactics as distribution methods for their malware, downloaders or malicious links. Some attacks are highly targeted against one individual or organization, a technique known as spear-phishing, but others are larger, broader campaigns. Email is easy to propagate and from many perspectives requires the fewest skills.

10. <https://www.nytimes.com/2009/09/15/technology/internet/15adco.html>

As we've noted before, phishing emails seek users' engagement to load malware into their system and, potentially, onto an organization's business network. These emails target consumers and business users with messages attempting to lure recipients into revealing confidential information, clicking links to unsafe sites, or opening malicious attachments. Once the threat actors have access to the system, they can use or find the confidential information and gain access to email, network, financial or other accounts.

Phishing emails often claim that they are from well-known financial institutions, shipping companies, social network sites, and online stores. The emails use enticing offers, information about popular topics, and notices that appear to require urgent attention. The emails also use the social-engineering techniques that attempt to lure users into opening attachments, clicking links to dangerous sites, and downloading malware.

Malicious attachments come in many formats, including PDF, ZIP, DOCX (Microsoft Word), and PPTX (Microsoft PowerPoint). In some cases, the threat actors direct users to enable macros or to open attachments and enable editing for them. Once enabled, the macros run a script that downloads and launches a malicious executable file from an external server. This executable can often encrypt data on the infected machine, contact its command and control, and potentially exfiltrate the victim's data.

Remote Desktop Protocol (RDP)

IT teams know RDP as the Microsoft protocol that facilitates remote connections to other computers. This connection usually occurs over TCP port 3389. RDP provides network access over an encrypted channel and allows users to remotely control Microsoft Windows devices. The basic capability of RDP is to transmit (1) the monitor (output device) from the remote endpoint or server to the RDP client and (2) the keyboard and mouse controls from the client to the remote endpoint or server. RDP also provides a GUI.

RDP is used to allow employees to access their office computers from endpoints outside the company. RDP comes with Microsoft Windows and supports Apple Macs. It is the standard protocol for many companies, because it allows team members to work from home, a capability especially important to companies during the pandemic.

RDP has become a highly effective and dangerous attack vector. Several years ago, one study noted that over 10 million online machines were configured with an open port, 3389. It has become a simple matter for threat actors to use search engines, such as Shodan, to locate these devices.

Threat actors can gain access to RDP servers by using default passwords on servers that have not been updated. Alternatively, the actors can use brute-force techniques to break in, or they can use open-source password crackers.

After the actors get in and escalate their privileges to those of an administrator, they can gain full control of a machine and encrypt files. They can also exploit vulnerabilities in the Microsoft RDP client, Free RDP (an open-source RDP client on GitHub), or RDesktop (an open-source RDP client that is a default RDP client in Kali Linux).

RDP is an administrative challenge for many small-size and medium-size businesses. In some cases, the RDP server is deployed and exposed to the Internet, and the IT team are either completely unaware of this or, if they are aware, fail to update or patch the RDP servers for years.

USB Memory Sticks

USB sticks have been used to distribute many types of malware, including ransomware. Threat actors leave USB drives in coffee shops, airports, mailboxes, and corporate lounges, for unsuspecting targets to pick up and use. Once a weaponized USB drive is inserted into a computer, the ransomware encrypts files on the device and propagates within the network.



NIST's Cybersecurity Framework Profile for Ransomware Risk Management

In June 2021, the NIST published a preliminary draft of NISTIR 8374.¹¹ The report defines a Ransomware Profile and identifies the security objectives specified as part of the NIST Cybersecurity Framework to support the prevention of, response to, and recovery from ransomware events. The Ransomware Profile can be used as a guide for managing risk and gauging an organization's level of readiness to mitigate ransomware threats and to react to the impact they cause.

NIST's National Cybersecurity Center of Excellence (NCCoE) has produced additional reference materials intended to support mitigation of ransomware threats. These references include:

- **NIST Special Publication (SP) 1800-26, Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events**¹² addresses how an organization can handle an attack when it occurs, and what capabilities it needs to have in place to detect and respond to destructive events.
- **NIST SP 1800-25, Data Integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events**¹³ addresses how an organization can work before an attack to identify its assets and potential vulnerabilities and remedy the discovered vulnerabilities to protect these assets.
- **NIST SP 1800-11, Data Integrity: Recovering from Ransomware and Other Destructive Events**¹⁴ addresses approaches for recovery should a data integrity attack be successful.
- **Protecting Data from Ransomware and Other Data Loss Events**¹⁵ is a guide for managed service providers to conduct, maintain, and test backup files that are critical to recovering from ransomware attacks.

CISA's New Ransomware Readiness Assessment

On June 30, 2021, CISA released a new Ransomware Readiness Assessment (RRA) module in its Cyber Security Evaluation Tool (CSET). CSET¹⁶ is a software tool that guides companies through a step-by-step process of evaluating their cybersecurity practices. CSET is flexible and can be applied to information technology as well as industrial control system networks and assets. By using many recognized government and industry standards and recommendations, companies can perform a deep evaluation of their cybersecurity posture.

The RRA is a self-assessment packaged as a tiered set of best practices for helping organizations assess their readiness to deal with ransomware incidents. CISA

11. <https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf>

12. <https://doi.org/10.6028/NIST.SP.1800-26>

13. <https://doi.org/10.6028/NIST.SP.1800-25>

14. <https://doi.org/10.6028/NIST.SP.1800-11>

15. <https://www.nccoe.nist.gov/sites/default/files/library/supplemental-files/msp-protecting-data-extended.pdf>

16. <https://github.com/cisagov/cset/releases/tag/v10.3.0.0>



has customized the RRA to different levels of readiness and is thus useful to any organization, at any level of cybersecurity maturity. The RRA:

- Helps companies evaluate their cybersecurity posture against ransomware by using recognized standards and best practices structured in a highly systematic, disciplined, and repeatable manner.
- Guides companies through a systematic process for evaluating their network security practices against the rapidly evolving ransomware threat.
- Provides an analysis dashboard with graphs and tables.

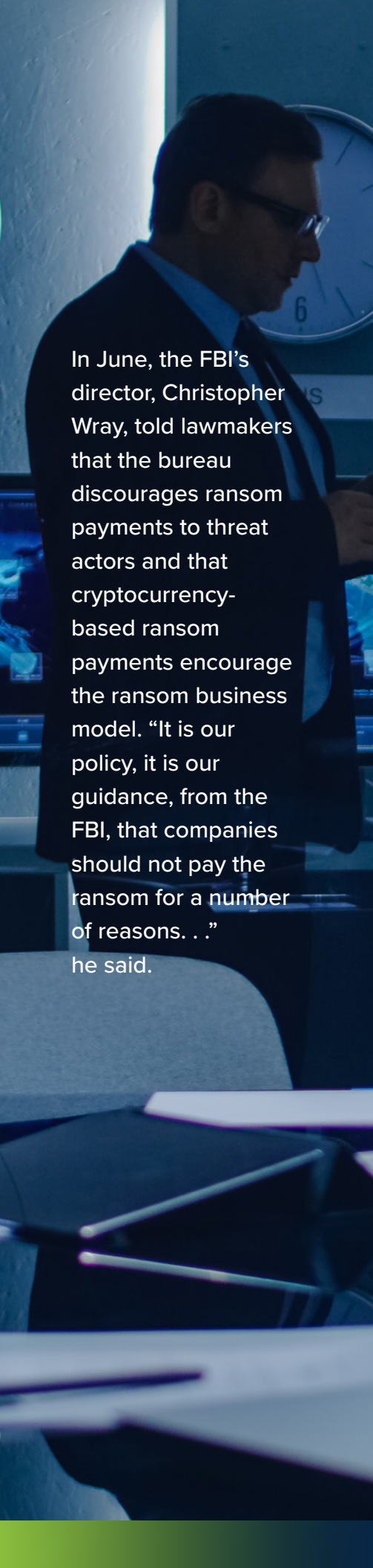
CISA has also brought up a new, highly informative section on ransomware:

<https://www.cisa.gov/stopransomware>.

Ransomware Mitigations

Practicing the following measures can help a company lower its vulnerability to a ransomware attack:

- Require multi-factor authentication for access to IT assets and applications. Revalidate authentication every time access is required for a new session.
- Use spam filters to prevent phishing emails and executable files from reaching end users. Doing this can stop many known malicious URLs early in the attack chain.
- Train users on handling phishing emails. Instruct users not to visit malicious websites, open malicious attachments, or enable macros in Microsoft Office attachments. If users are interested in a website, they must navigate there without using the links embedded in emails. This will greatly reduce the risks associated with ransomware delivered via malspam.
- Filter network traffic with DNS security to prohibit ingress and egress communications with known malicious IP addresses. Prevent users from accessing malicious websites by implementing block lists and allow lists. Some actors have malicious domains or URLs generated automatically; others create malicious IP addresses mere hours before sending phishing emails. Software that detects these algorithmically generated indicators of compromise can help protect against ransomware infections from newly created or registered malicious websites.
- Update software regularly. Most exploits can be eliminated by installing the supplier's latest updates.
- Limit access to resources over networks, especially by restricting RDP. Make sure RDP passwords have been changed from the default setting. If RDP is deemed operationally necessary, restrict the originating sources and require multi-factor authentication.
- Run regular scans with antivirus programs that use frequently updated signatures. Use machine learning–based tools to identify viruses and other malware that is based on users' behavior.
- Set a vulnerability scanner to run continuously, and run penetration tests regularly. Recent changes in configuration or the installation of updates can cause or expose vulnerabilities.



In June, the FBI's director, Christopher Wray, told lawmakers that the bureau discourages ransom payments to threat actors and that cryptocurrency-based ransom payments encourage the ransom business model. "It is our policy, it is our guidance, from the FBI, that companies should not pay the ransom for a number of reasons. . ."

he said.

- Disable macro scripts in Microsoft Office files transmitted via email.
- Implement an allowed-application listing, which lets systems execute programs known and explicitly permitted by security policy.
- Establish controls to prevent programs from executing from locations often used by ransomware. These locations include temporary folders that support popular internet browsers and compression/decompression programs. One example is the AppData/LocalAppData folder.
- Ensure that nothing in your networks is communicating with Tor. Refer to the Government Joint Cybersecurity Advisory AA20-183A: Defending Against Malicious Cyber Activity Originating from Tor.¹⁷
- Deploy signatures that would allow you to detect and block inbound connections from Cobalt Strike servers and other post-exploitation tools.

CISA and FBI Discourage Paying Ransoms

Paying a ransom emboldens an adversary to target more organizations, and it encourages other criminal actors to distribute ransomware and fund illicit activities. Also, paying a ransom does not guarantee that the targeted organization will recover its files and assets.

Insurers Might Drop Ransomware Coverage

AXA is a French insurance group that regularly ranks in the top five globally on net premiums written and other metrics.¹⁸ In June, the group announced¹⁹ that it would stop selling, in France, cyber insurance policies that would reimburse customers for extorted ransomware payments. Because AXA is an insurance market leader, its actions might signal the beginning of a larger trend to reduce the incentives for threat actors. Most companies do not have a discretionary budget set aside for millions in ransom payments, so they cannot afford to appease threat actors' ransom demands.

AXA suspended the option in response to the concerns raised by French justice and cybersecurity officials. In 2020, the impact of ransomware in France has been estimated in billions of U.S. dollars.

As the ransom amounts increase in the wake of the recent barrage of attacks, this creates challenges for the insurance industry. Oren Wortman, Managing Director²⁰ of the National Cyber Practice of Beecher Carlson Insurance Services, LLC, noted, "We have now seen, with our clients, ransoms paid in excess of \$10 million, with demands as high as \$40, \$50 and \$60 million. There are insurers out there who are blanket not writing any new business. There are insurers who are dropping business. And there are insurers who are completely excluding health care, public sector and higher education."²¹

17. <https://us-cert.cisa.gov/ncas/alerts/aa20-183a>

18. <https://www.insurancejournal.com/news/national/2021/01/05/596065.htm#>

19. <https://www.zdnet.com/article/axa-pledges-to-stop-reimbursing-ransom-payments-for-french-ransomware-victims/>

20. <https://beecher Carlson.com/company-news/national-cyber-practice-oren-wortman-managing-director/>

21. <https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks>



The Federal Government Steps up on Cybersecurity

This past quarter, we saw a significant increase in the federal government's activity focused on cybersecurity. In April, the Federal Reserve chairman, Jerome Power, said he was more worried about the risk of a large-scale cyberattack than another financial crisis such as that experienced in 2008. Power noted, "The world changes. The world evolves. And the risks change as well. And I would say that the risk that we keep our eyes on the most now is cyber risk." Power commented that this concern was shared by multiple governments and private businesses, particularly in finance.

Shortly after Jerome Power's comments, President Biden signed an [Executive Order improving cybersecurity defenses](#) in response to the Solar Winds attack and other attacks delivered by foreign threat actors. This Executive Order is a strong move toward modernizing cybersecurity defenses by protecting federal networks and improving information-sharing between the U.S. government and the private sector.

Anne Neuberger, President Biden's Deputy National Security Advisor for Cyber and Emerging Technology, has recently noted, "The threats [ransomware] are serious and they are increasing." Neuberger further wrote, "The private sector also has a critical responsibility to protect against these threats. All organizations must recognize that no company is safe from being targeted by ransomware, regardless of size or location. To better understand your risk, business executives should immediately convene their leadership teams to discuss the ransomware threat and review corporate security posture and business continuity plans to ensure you have the ability to continue or quickly restore operations."


In June, Energy Secretary Jennifer Granholm raised interest in more public-private sector cooperation on cyber defense. When asked whether the United States' foreign adversaries have the capability to use cyber intrusions to shut down the country's power grid, she said, "Yes, they do."²²

22. <https://www.marketwatch.com/story/energy-secretary-cites-risk-of-cyberattacks-crippling-u-s-power-grid-01623011242>

In June, Justice Department officials cautioned U.S. business leaders to prepare for an increasing onslaught of ransomware attacks. The Justice Department's efforts to organize a coordinated response have taken on an almost war-room level of effort as they seek to rally businesses to prepare for these increased attacks. In a move designed to improve the effectiveness of the federal government's tracking of online criminals, Deputy Attorney General Lisa Monaco issued an internal memo directing U.S. prosecutors to report all ransomware investigations they might be working on. The memo cites ransomware as an urgent threat to the nation's interests.

The tracking effort is expansive. It covers the DOJ's pursuit of not only ransomware criminals but also of the cryptocurrency tools they use to receive payments, the automated computer networks they use to spread ransomware, and the online marketplaces they use to advertise or sell malicious software. The DOJ's directive requires U.S. attorneys' offices to file internal reports on every new ransomware incident they hear about.

The attacks we see in the news are only the tip of an iceberg. Monaco has been on point for the DOJ's efforts against ransomware threat actors. She noted that the massive attacks against Colonial Pipeline and JBS USA were representative of the many ransomware attacks taking place every day.

A hand is shown typing on a keyboard in a dark, dimly lit environment. A glowing blue padlock icon is superimposed over the hand, and a glowing blue password field with asterisks is visible below it. The background is dark with some blurred light sources, and there are some glowing blue lines and shapes floating in the air, suggesting a digital or cyber environment.

“We must enhance and centralize our internal tracking of investigations and prosecutions of ransomware groups and the infrastructure and networks that allow these threats to persist,” Monaco wrote. She also noted “to the CEOs around the country, you’ve got to be on notice of the exponential increase of these [ransomware] attacks.”

NSA's and CISA's Guidance on DNS Security

DNS is key to the foundational security stack for enterprise and government. In 2021, the NSA and CISA have gone on record by recommending²³ that every agency, organization, and enterprise leverage the existing DNS protocol and architecture by using a protective domain name service (PDNS) service.²⁴ The information sheet *Selecting a Protective DNS Service*²⁵ details the benefits and risks of using DNS security, and it assesses several commercial PDNS providers according to their reported capabilities.

The Domain Name System (DNS) translates domain names into Internet Protocol addresses. DNS provides an opportunity to learn and control what resources a user is accessing on the network; this is the first step in an effort to figure out the user's intent. Based on the domain the user traffic is destined for, DNS knows the service being accessed.

PDNS, as defined by the NSA and CISA, is a security control that uses existing DNS protocols and architecture to analyze DNS queries and mitigate threats. Its core capability is to leverage various open-source, commercial, and governmental threat feeds to categorize domain information and to block queries to identified and suspected malicious domains. This capability provides defenses at various points of the network-exploitation lifecycle, and it addresses phishing, malware distribution, command and control, domain generation algorithms, and content filtering. PDNS can log and save suspicious DNS queries and block responses, thus delaying or preventing malicious activities—such as a ransomware that locks victims' files—while enabling an organization to investigate the attack by using those logged DNS queries.

The foundational security of Infoblox's BloxOne® Threat Defense provides a comprehensive DNS security capability. Infoblox received 100 percent of the performance score according to the criteria defined by NSA. For details, please see Table 1. For complete information, please see the latest version of the NSA and CISA document.²⁶

23. <https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2523771/nsa-and-cisa-release-cybersecurity-information-on-protective-dns/>

24. <https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2523771/nsa-and-cisa-release-cybersecurity-information-on-protective-dns/>

25. https://media.defense.gov/2021/Mar/03/2002593055/-1-1/0/CSI_PROTECTIVE%20DNS_UOO117652-21.PDF

26. https://media.defense.gov/2021/Mar/03/2002593055/-1-1/0/CSI_PROTECTIVE%20DNS_UOO117652-21.PDF

NSA & CISA Listed Protective DNS Performance Attributes Based on Reported Capabilities	Infoblox BloxOne Threat Defense Cloud
Blocks malware domains	✓
Blocks phishing domains	✓
Malware Domain Generation Algorithm (DGA) protection	✓
Leverages machine learning or other heuristics to augment threat feeds	✓
Content filtering	✓
Supports API access for SIEM integration or custom analytics	✓
Web interface dashboard	✓
Validates DNSSEC	✓
DoH/DoT capable	✓
Enables customizable policies by group, device or network	✓
Deploys across hybrid architectures	✓

Table 1: Criteria listed by NSA and CISA for a protective DNS service

Tracking Cybersecurity and Data Privacy Regulation

The Digital Operational Resilience Act (DORA) is currently in consultation and due to come into force in January 2022. This new regulation for financial services firms in the United Kingdom and Europe covers operational resilience from a technology perspective.²⁷

Compliance requirements generate large demands on organizations' data privacy and cybersecurity, regulation of which continues to grow at the municipal, state, and federal levels, in the United States and worldwide.

Hundreds of bills or resolutions that involve cybersecurity are under consideration. The legislation centers on:

- The implementation of training programs on cybersecurity, incident response, and formal security standards and policies
- Creating incentives and programs for education and training on cybersecurity
- Addressing or regulating cybersecurity insurance
- The formation of groups, commissions, or agencies to further advise and direct cybersecurity policies and advise organizations on important cybersecurity-related issues

As in the past quarter, bills will continue to move 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 that impact state and local government.

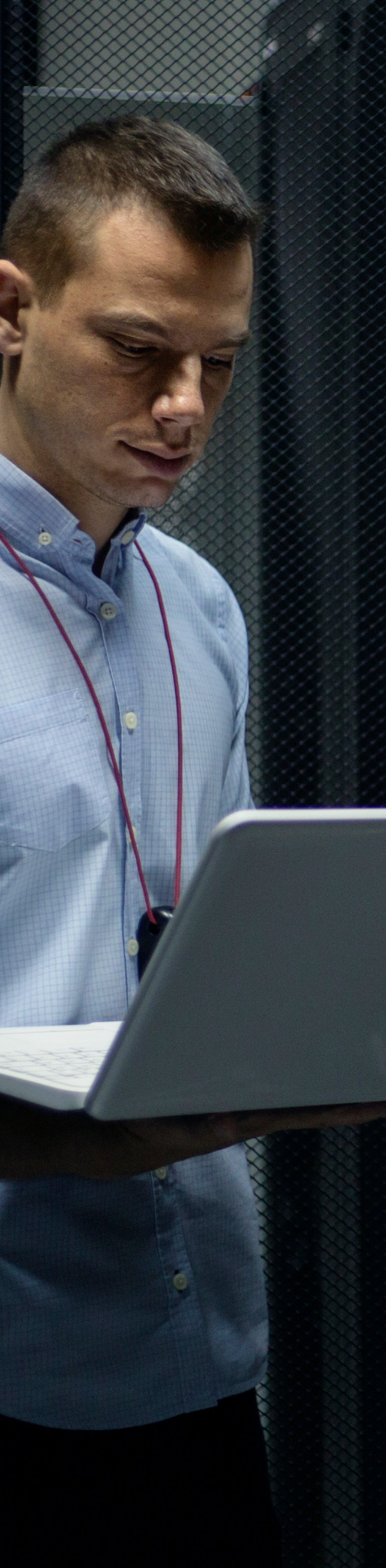
27. <https://www.google.com/url?q=https://www.paconsulting.com/newsroom/expert-opinion/ft-global-risk-regulator-what-firms-can-expect-from-dora-9-february-2021/&sa=D&source=editors&ust=1626233792147000&usq=AOvVawOyCFtqy7LPNAsMWzZ7MOhv>

S.1065 State Cyber Resiliency Act

- This bill was introduced to the Senate on April 8, 2019. The bill establishes the State Cyber Resiliency Grant Program to assist state, local, and tribal governments in preventing, preparing for, protecting against, and responding to cyber threats.
- Under this program, the Department of Homeland Security may award grants to a state for the development and implementation of an active cyber-resiliency plan. Such plan must be tailored to achieve specific objectives, including:
 - Enhancement of the response and resiliency of computer networks, industrial control systems, and communications systems against cybersecurity threats or vulnerabilities
 - Implementation of continuous vulnerability assessments and threat mitigation practices
 - Adoption of cybersecurity best practices by entities performing cybersecurity functions within a state
 - Confirmation that continuity of communications and data networks would be maintained in the event of a catastrophic disruption of such communications or networks

S.1846 State and Local Government Cybersecurity Act of 2019

- This bill was passed by the Senate on November 21, 2019.
- This bill provides for collaboration between the Department of Homeland Security (DHS) and state, local, tribal, and territorial governments, as well as corporations, associations, and the general public, regarding cybersecurity. The bill also provides for collaboration with foreign, as well as domestic, governmental agencies or entities, or corporations or associations.
- The bill expands DHS responsibilities through grants and cooperative agreements, including provision of assistance and education related to cyber threat indicators, defensive measures and cybersecurity technologies, cybersecurity risks, incidents, analysis, and warnings.
- The bill requires the National Cybersecurity and Communications Integration Center to coordinate with entities such as the Multi-State Information Sharing and Analysis Center to (1) conduct exercises, (2) provide operational and technical cybersecurity training, and (3) promote cybersecurity education and awareness.
- DHS may establish an initiative to enhance efforts to deploy technical or analytic capabilities or services that utilize classified cyber threat indicators or intelligence to detect or prevent malicious network traffic on unclassified non-federal information systems.



H.R.5823 State and Local Cybersecurity Improvement Act

- This bill was passed by the House of Representatives on September 30, 2020.
- This bill establishes a grant program and places requirements on CISA with respect to certain cybersecurity risks and threats. Specifically, CISA shall distribute grants to states for addressing cybersecurity risks and threats to the information systems of state, local, tribal, or territorial governments. A state applying for such a grant must (1) submit a cybersecurity plan for approval, and (2) establish a cybersecurity planning committee to assist with developing and implementing the state's cybersecurity plan and determining the effective funding priorities for the grant.
- CISA must establish a State and Local Cybersecurity Resiliency Committee whereby state, local, tribal, and territorial governments can advise CISA on their cybersecurity needs. In addition, CISA must develop and make publicly available a Homeland Security Strategy to Improve the Cybersecurity of State, Local, Tribal, and Territorial Governments that provides recommendations regarding how the federal government should support and promote the ability of such governments to protect against, respond to, and recover from cybersecurity risks, threats, and incidents. Further, CISA must develop a resource guide to assist officials of such governments with cybersecurity risks, threats, and incidents.
- CISA must also conduct a study to assess the feasibility of implementing a short-term rotational program for the detail of approved state, local, tribal, and territorial government employees in cyber workforce positions to the agency.

Security Breach Notification Laws

Security breach notification laws continue to get passed on a state-by-state basis. All 50 states, the District of Columbia, and U.S. territories have enacted legislation that requires private or governmental entities to notify individuals about data breaches that involve personally identifiable information.

Security breach laws typically have provisions that specify the following:

- Which businesses, data or information brokers, government entities, and other entities must comply with the law
- The definitions of personal information, such as a person's name combined with the SSN, driver's license or state ID, or account numbers
- What constitutes a breach, such as unauthorized acquisition of data
- Requirements for a notice, such as the timing or method of the notice, and who must be notified
- Exemptions, such as those for encrypting information

Q2 2021 Cyber Campaign Briefs and Cyberthreat Alerts

Malspam Campaign Spoofing Waybill Delivers NanoCore RAT

On June 21, Infoblox observed a malicious email campaign whose messages deliver NanoCore, a sophisticated remote access trojan (RAT). This malware was first discovered in 2013, when it was being sold in underground forums. Threat actors spread NanoCore mainly via malspam campaigns, by using phishing emails that contain a variety of attachments, such as ZIP and Microsoft Office files. Once executed, the malware allows the threat actors to remotely access the victim's machine, steal user information, and then send it to the command and control (C&C) servers operated by the actors. NanoCore has been observed in attacks on high-value targets in Asia, Europe, and the Middle East.

[Read the Full Brief →](#)

Hancitor Downloads Infostealers

From June 9 to 17, Infoblox observed multiple malspam campaigns that used DocuSign-themed lures. The malspam enticed users to download and open Microsoft Word documents with malicious macros that installed embedded copies of the trojan downloader Hancitor. The existence of these campaigns was independently corroborated by multiple external sources. Hancitor targets businesses and individuals around the world. Threat actors distribute it via malspam sent by compromised servers in the United States, Japan, Canada and many other countries.

[Read the Full Brief →](#)

Shathak Pushes IcedID Banking Trojan

On June 2, security researcher Brad Duncan reported on a malspam campaign in which the threat actor Shathak (aka TA551) was distributing the IcedID banking trojan. This trojan uses web injection and redirection attacks to steal banking credentials, credit cards, and other financial information from victims who believe they are entering their information into a secure website. In November 2020, we reported on the IcedID campaign in which Shathak distributed the malware via Japanese language malspam. In July 2020, we published a brief on a campaign wherein the threat actors used a Valak downloader to deliver IcedID.

[Read the Full Brief →](#)

RemcosRAT Malspam Campaign Spoofs UAE Machinery Company Correspondence

On May 23, we observed a malspam campaign distributing a ZIP file containing Remcos, a remote access trojan (RAT) designed to remotely control a victim's computer. The campaign's emails attempted to gain the victims' trust by impersonating Al Salehi Machinery & Equipment Repairing, a legitimate company in the United Arab Emirates. We have reported on various Remcos campaigns, including those that distributed the malware via malicious RTF files (in 2019) and XLS files (in 2020).

[Read the Full Brief →](#)

Cyberthreat Advisory - Nobelium Campaigns and Malware

On May 27 and 28, Microsoft published two reports on NOBELIUM, the threat actor behind the December 2020 supply chain attacks on SolarWinds' Orion platform. The first report detailed an ongoing spear-phishing campaign that leveraged a variety of techniques to distribute a Cobalt Strike Beacon payload that allows NOBELIUM to remotely control the targeted system through an encrypted network tunnel. The second report detailed four tools that were part of NOBELIUM's unique infection chain in that campaign: EnvyScout, BoomBox, NativeZone, and VaporRage.

[Read the Full Brief →](#)

Graftor Adware Still Circulating

On May 21, Infoblox observed a malicious spam campaign delivering Graftor malware via malicious file attachments. The threat actors used a generic invoice theme to lure victims into opening a weaponized Microsoft Excel spreadsheet. Graftor, aka LoadMoney, is a family of adware that has been used by threat actors for more than nine years. Past versions of Graftor were capable of browser hijacking, injecting advertising banners, installing unwanted applications, changing a user's homepage and search provider, and launching adware. Past versions also had anti-detection capabilities, such as antivirus and sandbox detection.

[Read the Full Brief →](#)

Biotech-Themed Malspam Drops BitRAT

On May 10, Infoblox observed a malicious email campaign that used weaponized Microsoft Excel spreadsheets (XLS) that exploited CVE-2017-11882 to deliver BitRAT, a remote access trojan (RAT). BitRAT, first observed in late 2020, is a relative newcomer to the malware scene. Poor coding practices in the malware indicated that its developers were inexperienced, because large sections of the code appear to be copied and pasted from another trojan, TinyNuke, as well as from a variety of open-source projects.

[Read the Full Brief →](#)

Cyberthreat Advisory: DarkSide Ransomware Attack on Colonial Pipeline

On May 11, CISA published an analytic report, AA21-131A, which detailed a ransomware attack on Colonial Pipeline, an important infrastructure entity in the U.S. The threat actors deployed DarkSide ransomware against the company's IT infrastructure, causing the company to take the precautionary measure of shutting down 5,550 miles of the pipeline, which left fuel stranded on the Gulf Coast. Although first observed in the wild in August 2020, DarkSide ransomware emerged in November 2020, on XSS, a popular Russian-language hacker forum.

[Read the Full Brief →](#)

Malspam Delivering Agent Tesla Keylogger Spoofs Email Addresses of Petroham Oil & Gas Companies

Between April 3 and 5, Infoblox observed a malicious spam campaign distributing weaponized Microsoft Excel spreadsheets (XLS) that contain malicious macros intended to infect machines via the Agent Tesla keylogger. The threat actors used a spoofed email sender address to gain the targets' trust by impersonating Petroham Oil & Gas, a legitimate chemical and petrochemical company based in Abu Dhabi.

[Read the Full Brief →](#)

Cyberthreat Advisory: FiveHands Ransomware

On May 6, CISA published the analytics reports AR21-126A1 and AR21-126B2 about a newly discovered ransomware variant, FiveHands. The reports include details of the recent cyberattack that uses FiveHands, and they provide information on the tactics, techniques and procedures (TTPs), as well as a malware analysis of the 18 files used by threat actors. FireEye's Mandiant team has labeled the threat actors UNC2447. This sophisticated and financially motivated group and its affiliates have been active since May 2020 and targeting organizations in Europe and North America. UNC2447 uses FiveHands ransomware to exfiltrate victims' data and threaten the victims with media attention or with selling the stolen data on hacker forums if the victims do not pay the ransom.

[Read the Full Brief →](#)

Polish Language Malspam Campaign Delivers AveMaria Infostealer

Between April 25 and 30, Infoblox observed a malspam campaign distributing the AveMaria remote access trojan (RAT). The threat actors used email subject lines, written in Polish, to reference payment confirmations and to lure victims into downloading a malicious executable. Infoblox has previously reported on AveMaria in April 2019 and December 2020.

[Read the Full Brief →](#)



Post-Takedown Trickbot Activity

On April 25, Infoblox observed a phishing campaign that used a DocuSign lure and a malicious file attachment to infect victims' computers with the Trickbot banking trojan. Although Microsoft and other organizations disrupted the Trickbot botnet in October 2020, multiple sources have seen activity from the botnet since then. We have published several reports on Trickbot, including a Malicious Activity Report and Cyber Campaign Briefs.

[Read the Full Brief →](#)

Spoofed Vehicle Purchase Invoice Malspam Drops Formbook Infostealer

On April 12, Infoblox observed an email campaign distributing Formbook malware via Microsoft Office documents that contained malicious macros. Emails in this campaign lure victims into opening a spoofed purchase invoice from Hyundai and into enabling macros to access the document's content. In our reports, we have noted Formbook campaigns' tendency to use financial-themed lures and other urgent topics, such as the Coronavirus pandemic.

[Read the Full Brief →](#)

Agent Tesla Malspam Campaign Spoofs Bank Correspondence

From April 1 to 6, we observed a malspam campaign distributing a TAR file containing Agent Tesla, a remote access trojan (RAT) designed to steal information from a victim. The campaign's email subjects attempted to gain the victim's trust by impersonating the British bank Standard Chartered. Some of the emails claimed to offer advice from the bank and notified the recipient of a payment.

[Read the Full Report →](#)

Italian Economic Support–Themed Malspam Delivers Ursnif Banking Trojan

On March 30, Infoblox observed a malspam campaign using an economic support–themed message to lure Italian-speaking victims into opening a malicious attachment that delivers Ursnif, a widely distributed banking trojan. The tactics, techniques, and procedures (TTPs) we observed in this campaign are consistent with those described in recent reports on Ursnif.

[Read the Full Brief →](#)

The 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.



Powered by the
Infoblox Cyber Intelligence Unit

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 networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent 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

© 2021 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).

Infoblox 

