Infoblox

# Q3 | 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

The High Cost of a Data Breach ....................................................................6

Alert Fatigue and Overload ...........................................................................6

Healthcare Remains in the Bull's-Eye ...........................................................8

DHS's 60-Day Cybersecurity Sprints .........................................................10

CISA's Zero Trust Maturity Model: Comment Window Closed
October 1, 2021 ..........................................................................................12

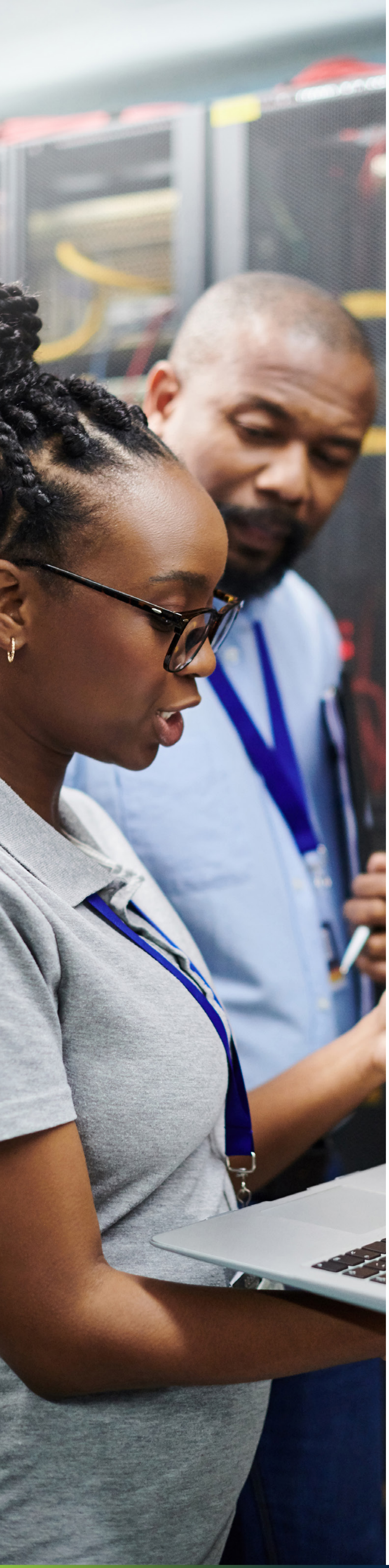
FBI's IC3 Industry Alerts for Q3 2021 .........................................................14

Alerts, Advisories, and Reports Published by the National
Security Agency and Central Security Service – Q3 2021 .........................17

Infoblox Threat Reports and Cyber Threat Alerts – Q3 2021 ..................20

The Infoblox Cyber Intelligence Unit .........................................................30

Infoblox Threat Intelligence .......................................................................30



# Executive Summary

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

The Q3 2021 report includes 30+ threat intelligence reports that we released to the public from July 1, 2021 to September 30, 2021. This quarter, we share a preview of our research into a healthcare data breach; cover the execution of the cybersecurity sprints being conducted by the United States Department of Homeland Security; discuss the rapid and important evolution of the Cybersecurity and Infrastructure Security Agency's Zero Trust Maturity Model; and summarize important IC3 industry alerts, advisories, and reports that the Federal Bureau of Investigation, National Security Agency, and Central Security Service published during this quarter.

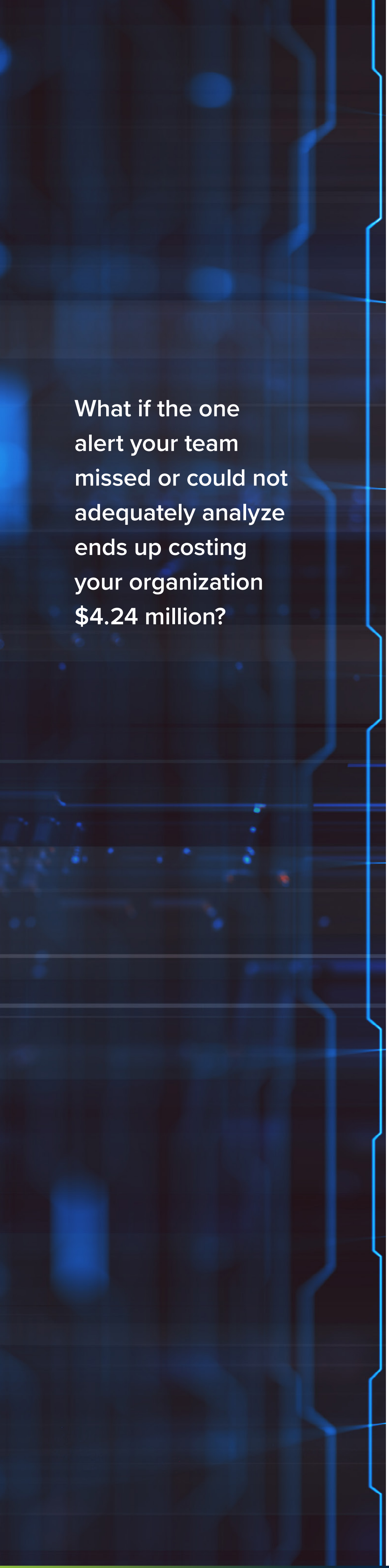
This publication supplements our original research and insight into the threats we observed leading up to and during this period of time. Our report includes a detailed analysis of advanced malware campaigns and of recent significant attacks. In some cases, we share and expand on original research published by other security firms, industry experts, and university researchers. We feel that timely information on cyber threats 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 threats under review.

During Q3 2021, the Infoblox Cyber Intelligence Unit (CIU) published the following reports on campaigns that delivered malware:

- Reply-Chain Threadjacking Campaign Delivers Squirrelwaffle Loader and Cobalt Strike
- Likely FIN7 Recon Campaign
- Fake Delivery Emails Deliver AsyncRAT
- XpertRAT Returns
- Hancitor Adds Second Redirect
- GuLoader Delivers Remcos RAT
- New Malware: Capturador Hijacker
- Hive Ransomware
- Fake Shipping Emails Deliver Ratty RAT
- OnePercent Group Ransomware Campaign

- “Urgent Report” Spam Drops Danabot Banking Trojan
- Update on the Attack on the Italian Regional Data Center
- Transfer-Themed Malspam Drops STRRAT
- New Spam Actor: EggshellCheetah
- Swift Payment-Themed Malspam Delivers Oski Stealer
- LemonDuck Trojan Delivers Cryptominers and Other Malware
- Cyber Threat Advisory: Attack on Italian Regional Data Center
- Infoblox Identifies New Threat Actor: WhiteSawShark and New Malware—HadLoader
- Purchase Order Malspam Delivers Snake Keylogger
- Cyber Threat Advisory: APT31 Targeting France
- Adult-Themed Mimail Worm Campaign Steals Victim Information
- Cyber Threat Advisory: U.S. Oil Pipeline Intrusion
- Cyber Threat Advisory: APT40 TTPs and Trends
- Spoofed Kazakh Malspam Delivers Neshta Infostealer
- Cyber Threat Advisory: SonicWall Vulnerability
- Fake Kaseya Patch Malspam Campaign
- Cyber Threat Advisory: Kaseya Ransomware Attack Update: Patch Available
- Cyber Threat Advisory: DarkSide Ransomware Variant
- Malspam RTF Files Drop Formbook Infostealer
- Cyber Threat Advisory: Kaseya REvil Ransomware Attack
- Fancy Bear Brute Force Attacks



What if the one alert your team missed or could not adequately analyze ends up costing your organization $4.24 million?

# The High Cost of a Data Breach

According to the Ponemon Institute's 2021 Cost of Data Breach Study, the average cost of a data breach in 2020 was an all-time high of $8.64 million in the United States and $3.83 million worldwide; in 2021, the latter was 10 percent higher, or $4.24 million.

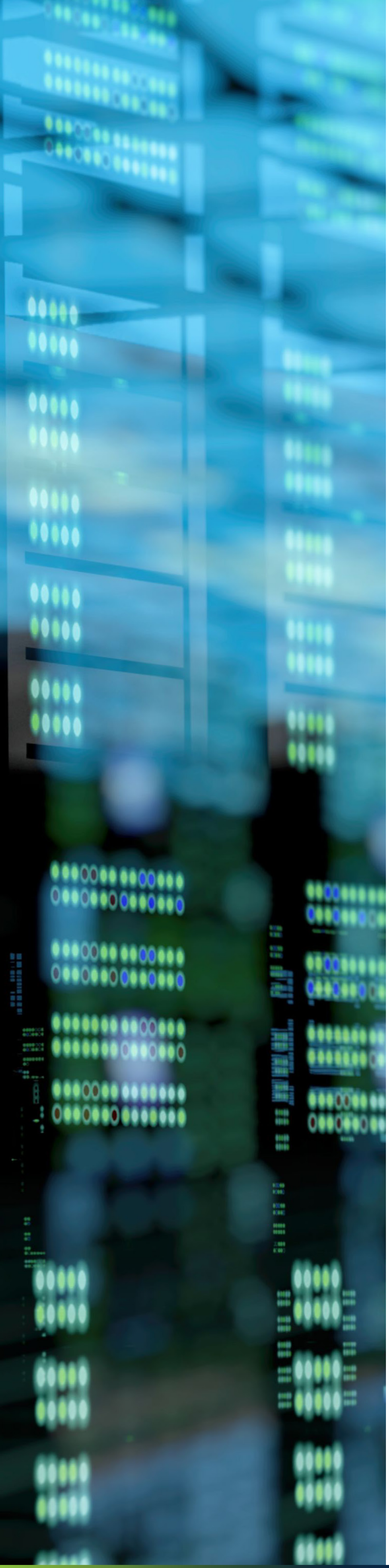
The report takes into account hundreds of factors, such as legal, regulatory and technical activities, loss of brand equity, customer turnover, and drain on employee productivity. Its findings are based on the data gathered from almost 3,500 interviews and 537 breaches across 17 countries and 17 industries.

# Alert Fatigue and Overload

A survey that Trend Micro published in mid-2021 polled more than 2,000 SOC analysts and decision makers from a variety of companies that operate in 21 countries and have more than 250 employees:

- **51 percent** of the respondents felt that their teams were being overwhelmed by the volume of alerts. These teams were spending as much as 27 percent of their time responding to and managing false positives.
- **55 percent** admitted that they were not entirely confident in their ability to prioritize and respond to the alerts.
- **43 percent** said they turn off alerts (occasionally or frequently) or just walk away from their computers.

> *"Cyber-security and SOC operations are typically described with playbooks and metrics wrapped around risk, security controls, alerts, vulnerabilities and attacker tactics, techniques and procedures… we need to equip them with the threat intelligence and automated ecosystem they need to more easily triage these threat volumes down to those incidents that truly require their attention."*
>
> **Anthony James, vice president of product marketing at Infoblox, Inc.**



During a recent RSA conference, Imperva surveyed 179 IT professionals to find out how different teams are dealing with their alert volumes. 55 percent of the respondents said they receive more than 10,000 alerts daily, and 27 percent reported receiving a staggering 1 million or more threat alerts daily. 53 percent of the respondents said that their organizations' analysts struggle to pinpoint which security incidents are critical and which are just noise. Responding to such a large number of requests is very difficult, but separating the actual threats from false-positives presents a challenge just as formidable. According to a 2021 survey conducted by the analyst firm Enterprise Strategy Group (ESG), cybersecurity operations are more difficult today than they were a mere two years ago, for the following reasons as stated by respondents:

- **41 percent:** Threat landscape is evolving and changing rapidly
- **35 percent:** There is more security data to collect and process
- **34 percent:** The volume of security alerts has increased
- **30 percent:** The attack surface has grown

According to the study, the proportion of the respondents highlighted the following as the biggest challenges attributed to monitoring alerts:

- **38 percent:** Filtering out the noise to give priority to real alerts
- **37 percent:** Implementing production processes to scale collection and analysis of security data
- **36 percent:** Processing and contextualizing threat intelligence data from multiple sources

Worse yet, what does the SOC team do with the alert volumes too high for their existing processes and systems?

Nothing.

An alarming 30 percent of respondents admitted to having flat-out ignored certain categories of alerts, 57 percent tuned their policies to reduce alert volume, while 4 percent actually turned off the alert notifications altogether. On a slightly more positive note, 10 percent said that they hire additional SOC engineers to help deal with these alerts.

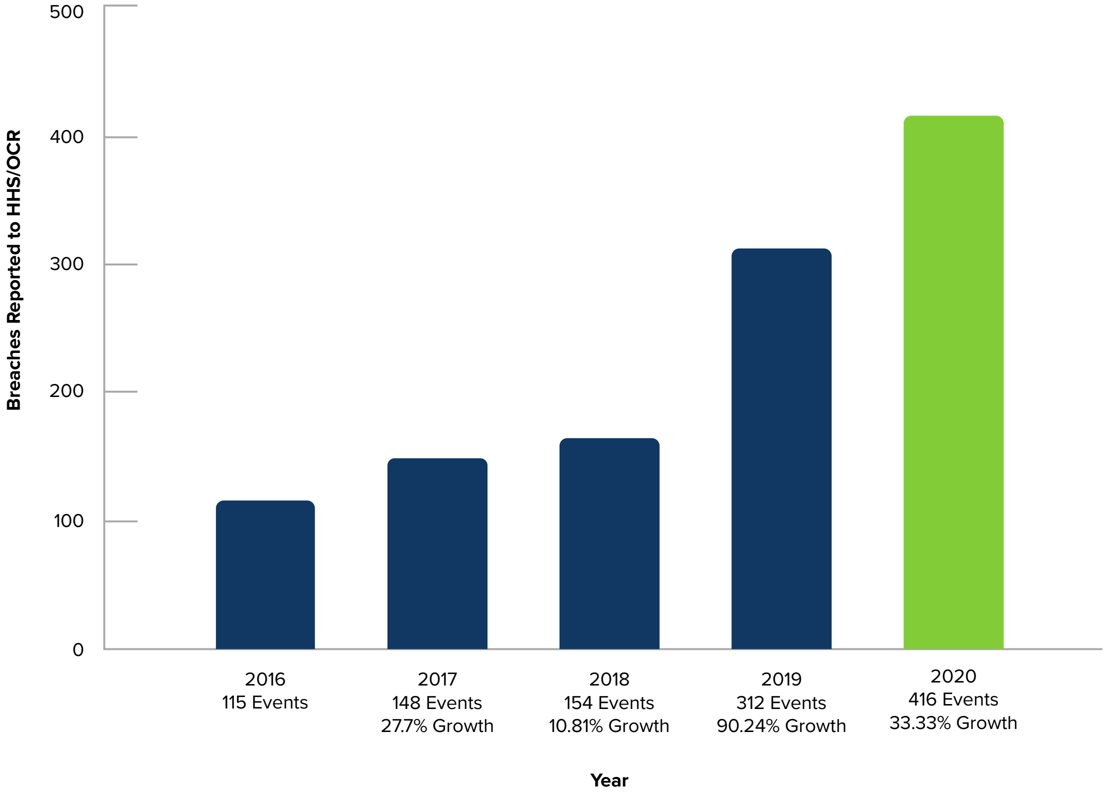
# Healthcare Remains in the Bull’s-Eye

Our annual Healthcare Cyber Trend Research Report provides analysis of the major healthcare data breaches directly attributable to cyber attacks in the United States. In January, we published the report for 2020, and our research team has already started reviewing the data for 2021. Our preliminary analysis tells us that the healthcare industry remains in high jeopardy from a rising tide of targeted cyber threats. We expect substantial increases in both the number of major data breaches (defined as impacting over 500 patient records and attributed to “IT/Hacking” by the reporting entity) and in the total number of patient records impacted. We expect that this increase has, in great part, been caused by ransomware, but confirmation will remain open until we perform more analyses.

In summary, our preliminary data analysis shows the following:

| Area of Comparison | 2020 Report: Full Year | Preliminary Data for 2021: Half Year Only |
|---|---|---|
| Number of major data breaches | 416 major data breaches were reported in 2020. This was 33 percent more than the 312 major data breaches reported in 2019. | 249 major data breaches were reported just in the first half of 2021. |
| Number of patient records impacted | 26,424,309 patient records were impacted by the major data breaches throughout the entire 2020. | 22,270,460 patient records were impacted by major data breaches just in the first half of 2021. |

The following chart shows the data we collected from 2016 to 2020. We expect this data to be eclipsed by the data we have collected in 2021.



# DHS's 60-Day Cybersecurity Sprints

The United States Department of Homeland Security (DHS) have been conducting a series of 60-day sprints. These are part of the DHS's initiative to mitigate the current issues related to ransomware, cybersecurity workforce, defense of industrial control systems, transportation systems and election infrastructure.

The first sprint addressed ransomware, which "now poses a national security threat," said DHS Secretary Alejandro Mayorkas at a virtual conference hosted by RSA on March 31, 2021. According to Mayorkas, the sprint included actions that would help organizations lessen the risk of falling victim to cyberattacks by engaging with industry and key partners, such as insurance companies. "We will strengthen our capabilities to disrupt those who launch them and the marketplaces that enable them," said Mayorkas. He also said that each cyber sprint would have a dedicated action plan within DHS, build off of existing efforts made by agencies, and focus on knocking down interagency roadblocks for cyber response. Mayorkas outlined the following six cyber sprints, which are now at various stages of completion, planning and execution:

## Ransomware: April 2021 - May 2021

This sprint focused on leveraging the Office of the Secretary to elevate the fight against ransomware, an increasingly devastating and costly form of malicious cyber activity that targets organizations of all sizes and across all sectors. Ransomware is malicious code that infects and paralyzes computer systems until a ransom has been paid. Individuals, companies, schools, police departments, hospitals and other critical infrastructures have been among the recent victims.

## Cyber workforce: May 2021 – June 2021

This sprint focused on building a more robust and diverse cybersecurity workforce. DHS cannot tackle ransomware and the broader cybersecurity challenges without talented and dedicated people who can help protect the nation's schools, hospitals, critical infrastructure and communities. To this end, DHS onboarded over 300 new cybersecurity employees and made 500 tentative job offers, which is 50 percent more offers than planned.

## Industrial control systems: July 2021 – August 2021

This sprint was driven by the White House Industrial Control Systems Cybersecurity Initiative, which aims to improve the resilience of industrial control systems. The attempted cyber attack on a water-treatment facility in Florida and the ransomware attack on Colonial Pipeline were powerful reminders of the substantial risks to be addressed.

## Transportation security: September 2021 – October 2021

During this sprint, the Secretary has focused specifically on the need to increase the cyber resilience of the U.S. transportation systems: aviation, railways, pipelines, and marine. The Transportation Security Agency (TSA), U.S. Coast Guard, and CISA are all part of DHS, and this presents a unique opportunity for the DHS to accelerate progress of this effort by leveraging each department's best practices and by deepening the collaboration with the U.S. Department of Transportation, various interagency stakeholders and industry.

## Election security: November 2021 – December 2021

This sprint will focus on cementing the resilience of the nation's democratic infrastructures and protecting the integrity of its elections. By leveraging the lessons learned from previous elections and the relationships CISA have built with local and state authorities across the country, this sprint will ensure that election security remains a top priority every year, not only during the election season.

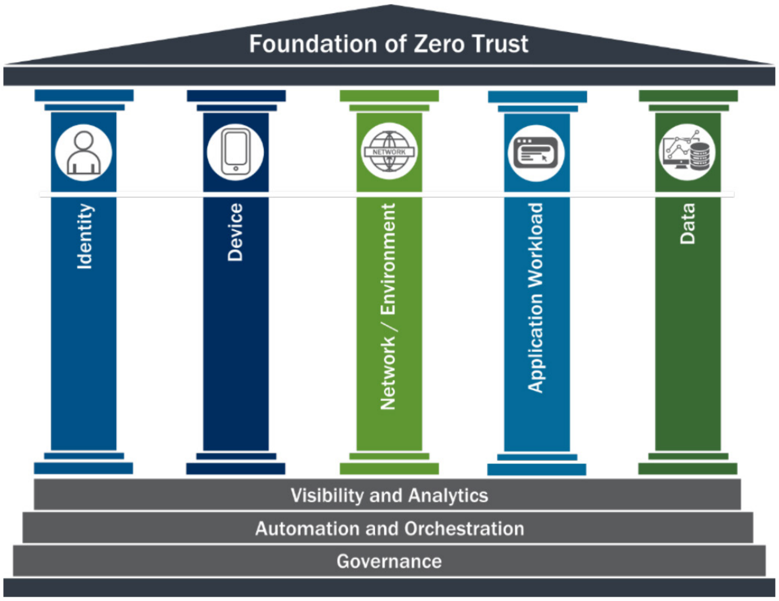
## Advancing international partnerships: January 2022 – February 2022

This sprint will encompass the department's international effort to implement the goals outlined in the CISA Global strategy and in the U.S. Coast Guard's Cyber Strategic Outlook. Most of the cybercrime-related investigations that the United States Secret Service, Immigration and Customs Enforcement, and Homeland Security investigations pursue every day have a transnational dimension and require cooperation with law enforcement partners around the globe.

# CISA's Zero Trust Maturity Model: Comment Window Closed October 1, 2021

From September 7 to October 1, CISA had a draft of its Zero Trust Maturity Model released to the public. The agency will update and publish the document according to the comments it received during this period.

The Zero Trust Maturity Model represents a gradient of implementation across five distinct pillars, where minor advancements can be made over time toward optimization. The pillars, depicted in the graphic below, include Identity, Device, Network, Application Workload, and Data. Each pillar also includes general details regarding Visibility and Analytics, Automation and Orchestration, and Governance. This maturity model is one of many paths towards zero trust.



As implementers transition towards optimal zero trust implementations, their solutions increase in reliance upon automated processes and systems, more fully integrate across pillars, and become more dynamic in their policy enforcement decisions. Each pillar can progress at its own pace and may be farther along than others, until cross-pillar coordination is required. Additionally, the interoperability and dependencies within the cross-pillar coordination must ensure compatibility. This allows for a gradual evolution to zero trust, distributing costs over time rather than entirely upfront. To facilitate migration, the Zero Trust Maturity Model gradient can be described using three stages, with increasing levels of protection, detail, and complexity for adoption, as outlined below. The following descriptions of each stage were used to identify maturity for each zero trust technology pillar and to provide consistency across the maturity model:

1. **Traditional:** manual configurations and assignment of attributes, static security policies, pillar-level solutions with coarse dependencies on external systems, least-function established at provisioning, proprietary and inflexible pillars of policy enforcement, manual incident response and mitigation deployment
2. **Advanced:** some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to predefined mitigations, increased detail in dependencies with external systems, and some least-privilege changes made according to posture assessments
3. **Optimal:** fully automated assignment of attributes to assets and resources, dynamic policies based on automated or observed triggers, assets that have self-enumerating dependencies for dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, and centralized visibility with historical functionality for point-in-time recollection of state

Other federal efforts related to the model are described in the following publications:

- National Institute of Standards and Technology Special Publication 800-207

  This document describes Zero Trust for enterprise security architects. It is meant to help them understand how Zero Trust applies to unclassified civilian systems, and it provides a road map for deploying Zero Trust architecture to an enterprise environment. This document is the product of a collaboration between multiple federal agencies and is overseen by the Federal Chief Information Officer Council.

- Department of Defense Zero Trust Reference Architecture

  This document describes the scope of the Department of Defense (DoD) Zero Trust Reference Architecture effort, and that is to determine the capabilities and integrations that can be used to successfully advance the DoD Information Network to an interoperable Zero Trust end-state. The architecture's design is focused on data but, to maximize interoperability, maintains loose coupling across services. This document will evolve as requirements, technology, and best practices evolve and mature.

- National Security Agency: Embracing Zero Trust Security Model

  This document explains the benefits of Zero Trust and the challenges of implementing it. It also discusses the importance of building a detailed strategy, dedicating the necessary resources, maturing the implementation, and fully committing to Zero Trust to achieve the desired results. The recommendations put forth in the document will help cybersecurity leaders, enterprise network owners, and administrators embrace this modern cybersecurity model.

# FBI's IC3 Industry Alerts for Q3 2021

## Cyber Criminal Actors Targeting the Food and Agriculture Sector with Ransomware Attacks – September 1, 2021

Ransomware attacks targeting the food and agriculture sector disrupt operations, cause financial loss, and damage the food supply chain. Ransomware may impact businesses across the sector: from small farms to large producers, from processors to manufacturers, and from markets to restaurants.

Cyber-criminals exploit network vulnerabilities to exfiltrate data and encrypt systems in a sector that is increasingly reliant on smart technologies, industrial control systems, and Internet-based automation systems.

Food and agriculture businesses victimized by ransomware lose money on ransom payments, lost productivity, and remediation expenses. In addition, they might lose proprietary information, personally identifiable information (PII), and their very reputation. Here are but a few examples of the damages sustained by food and agriculture businesses that fell victim to ransomware attacks:

- In July 2021, a bakery in the U.S. was attacked by Sodinokibi/REvil, which was deployed through software used by a managed service provider (MSP) of IT support. Due to lost access to its server, files and applications, the company had to halt its production, shipping, and receiving and had to shut down for approximately one week. The company could not fulfil customer orders on time, and its reputation suffered.

- In May 2021, cyber actors using a variant of the Sodinokibi/REvil ransomware compromised computer networks in the U.S. and overseas locations of a global meat processing company. This possibly resulted in exfiltration of company data and caused it to shut down some of its U.S.-based plants for several days. The temporary shutdown reduced the number of cattle and hogs slaughtered, caused a shortage of meat supply in the United States, and drove wholesale meat prices up as much as 25 percent.

- In March 2021, a U.S. beverage company suffered a ransomware attack that caused a significant disruption to its business operations, production, and shipping. To prevent further spread of the malware, the company took its systems offline, and this prevented the employees from accessing specific systems.

- In January 2021, a ransomware attack against a United States farm resulted in losses totalling approximately $9 million due to the temporary shutdown of operations. The unidentified threat actor was able to target the farm's internal servers by gaining administrator-level access through compromised credentials.

- In November 2020, a U.S.-based international food and agriculture business reported that due to a ransomware attack, it was unable to access multiple computer systems tied to its network. The attack was traced to the OnePercent Group, who used a phishing email to infect the company's administrative systems through a malicious zip file attachment. The cyber criminals downloaded several terabytes of data through its cloud service provider, and then encrypted hundreds of folders. The business did not pay the $40 million ransom and was able to successfully restore its systems from backups.

Read the Full Report ➔

## Top Routinely Exploited Vulnerabilities – July 28, 2021

This advisory was authored through a collaboration of the FBI, CISA, Australian Cyber Security Centre (ACSC), and National Cyber Security Centre (NCSC) of the United Kingdom. It provides details about the common vulnerabilities and exposures (CVEs) that cyber criminals have been exploiting since 2020.

Cyber criminals continue to exploit publicly known—and often dated—software vulnerabilities against broad target sets, including public and private organizations across the world. However, organizations can mitigate the vulnerabilities listed in this report, by applying the available patches to their systems and implementing a centralized patch-management system. The following were the top routinely exploited CVEs in 2020:

| Vendor | CVE | Type |
|---|---|---|
| Citrix | CVE-2019-19781 | Arbitrary code execution |
| Pulse | CVE-2019-11510 | Arbitrary file reading |
| Fortinet | CVE-2018-13379 | Path traversal |
| F5-Big IP | CVE-2020-5902 | Remote code execution (RCE) |
| MobileIron | CVE-2020-15505 | RCE |
| Microsoft | CVE-2017-11882 | RCE |
| Atlassian | CVE-2019-11580 | RCE |
| Drupal | CVE-2018-7600 | RCE |
| Telenik | CVE-2019-18935 | RCE |
| Microsoft | CVE-2019-0604 | RCE |
| Microsoft | CVE-2020-0787 | Elevation of privilege |
| Netlogon | CVE-2020-1472 | Elevation of privilege |

## 2021 CVEs

In 2021, cyber actors continue to target vulnerabilities in perimeter-type devices. In addition to mitigating the 2020 CVEs listed above, organizations should prioritize patching for the following CVEs:

- **Microsoft Exchange:** CVE-2021-26855, CVE-2021-26857, CVE-2021-26858 and CVE-2021-27065

  See CISA's alert Mitigate Microsoft Exchange Server Vulnerabilities.

- **Pulse Secure:** CVE-2021-22893, CVE-2021-22894, CVE-2021-22899 and CVE-2021-22900

  See CISA's alert Exploitation of Pulse Connect Secure Vulnerabilities.

- **Accellion:** CVE-2021-27101, CVE-2021-27102, CVE-2021-27103 and CVE-2021-27104

  See the Australia-New Zealand-Singapore-U.K.-U.S. Joint Cybersecurity Advisory Exploitation of Accellion File Transfer Appliance.

- **VMware:** CVE-2021-21985

  See CISA's Current Activity entry Unpatched VMware vCenter Software.

- **Fortinet:** CVE-2018-13379, CVE-2020-12812 and CVE-2019-5591

  See the CISA-FBI Joint Cybersecurity Advisory, APT Actors Exploit Vulnerabilities to Gain Initial Access for Future Attacks.

Read the Full Report →

# Alerts, Advisories, and Reports Published by the National Security Agency and Central Security Service – Q3 2021

The following advisories, info sheets, tech reports, and operational risk notices were issued in Q3 2021:

## CSI: Selecting and Hardening Remote Access VPN Solutions – September 28, 2021

Virtual private networks (VPNs) allow users to remotely connect to a corporate network via a secure tunnel. Through this tunnel, users can take advantage of the internal services and protections normally offered to on-site users, such as email/ collaboration tools, sensitive document repositories, and perimeter firewalls and gateways. Because remote access VPN servers are entry points into protected networks, they are targets for adversaries.

This joint NSA-CISA information sheet provides guidance on:

- Selecting standards-based VPNs from reputable vendors with a proven track record of quickly remediating known vulnerabilities and of following best practices for using strong authentication credentials
- Hardening the VPN by reducing the VPN server's attack surface through the following:
  - Configuring strong cryptography and authentication
  - Running only necessary features
  - Protecting and monitoring access to and from the VPN

## CSI: Conti Ransomware – September 22, 2021

This alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, version 9.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations. In typical Conti ransomware attacks, cyber criminals steal files, encrypt servers, and workstations and demand a ransom payment. To secure systems against Conti ransomware, the CISA, FBI and National Security Agency (NSA) recommend implementing the mitigation measures described in this alert, which include requiring multi-factor authentication (MFA), implementing network segmentation, and keeping operating systems and software up to date.

### CSI: Keeping Safe on Social Media – August 6, 2021

Social media sites and apps are great ways to connect and share information. User profiles, timelines, social media status, friend lists, and message services grant your contacts insights into your day-to-day activities. However, these sites can also provide adversaries with the critical information they need to disrupt your life and harm or harass you, your co-workers, or even your family members. The following guidance can better prepare you to protect against online threats.

Practicing good operations security (OPSEC) and using simple countermeasures will minimize the risks that come from using social media and will help you protect your critical information.

### NSA and CISA: Cybersecurity Technical Report: Kubernetes Hardening Guidance – August 3, 2021

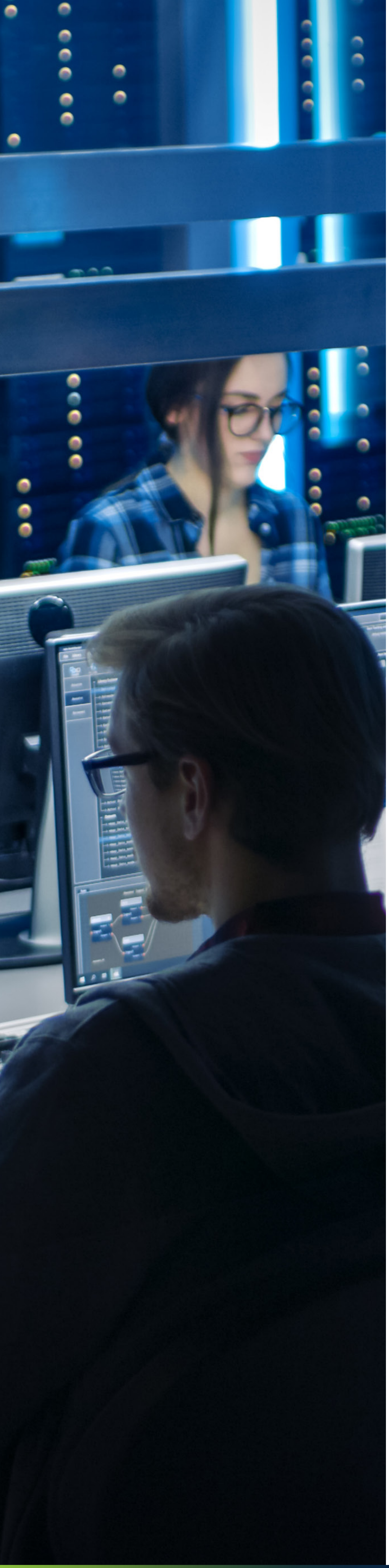
Kubernetes® is an open-source system that automates the deployment, scaling, and management of applications run in containers, and is it often hosted in a cloud environment.

This type of virtualized infrastructure offers more flexibility and benefits than offered by traditional, monolithic software platforms. However, securely managing everything from microservices to the underlying infrastructure introduces other complexities. The hardening-related guidance detailed in this report is designed to help organizations handle associated risks and enjoy the benefits of using this technology.

### CSI: Securing Wireless Devices in Public Settings – July 29, 2021

Telework has become an essential component of business, and many people are teleworking from home or during travel. While the owners of home networks can take steps to secure those networks, it can be difficult to ensure public networks (for example, conference or hotel Wi-Fi) are secure. Protecting personal and corporate data is essential at all times, but especially when teleworking in public settings. To ensure data, devices and login credentials remain secure and uncompromised, cyber security is a crucial priority for users and businesses. This includes identifying higher-risk public networks and implementing security best practices while in public settings, whether connecting laptops, tablets, mobile phones, wearable accessories, or other devices with the ability to connect to the internet.

This report gives users from the National Security Sytstem (NSS), Department of Defense (DoD), and Defense Industrial Base (DIB) the best practices for securing devices when conducting business in public settings.



CSA: Chinese State Sponsored Cyber TTPs – July 19, 2021

The National Security Agency, Cybersecurity and Infrastructure Security Agency (CISA), and Federal Bureau of Investigation (FBI) assess that People's Republic of China state-sponsored malicious cyber activity is a major threat to U.S. and Allied cyberspace assets. Chinese state-sponsored cyber actors aggressively target U.S. and allied political, economic, military, educational, and critical infrastructure (CI) personnel and organizations to steal sensitive data, critical and emerging key technologies, intellectual property, and personally identifiable information (PII). Some target sectors include managed service providers, semiconductor companies, the Defense Industrial Base (DIB), universities, and medical institutions. These cyber operations support China's long-term economic and military development objectives.

This Joint Cybersecurity Advisory (CSA) provides information on tactics, techniques, and procedures (TTPs) used by Chinese state-sponsored cyber actors. This advisory builds on previous NSA, CISA, and FBI reporting to inform federal, state, local, tribal, and territorial (SLTT) government, CI, DIB, and private industry organizations about notable trends and persistent TTPs through collaborative, proactive, and retrospective analysis.

CSA: Russian GRU Global Brute Force Campaign – July 1, 2021

Since at least mid-2019 through early 2021, Russian General Staff Main Intelligence Directorate (GRU) 85th Main Special Service Center (GTsSS), military unit 26165, used a Kubernetes cluster to conduct widespread, distributed and anonymized brute force access attempts against hundreds of government and private sector targets worldwide. GTsSS malicious cyber activity has previously been attributed by the private sector using the names Fancy Bear, APT28, Strontium and a variety of other identifiers. The 85th GTsSS directed a significant amount of this activity at organizations using Microsoft Office 365 cloud services; however, it also targeted other service providers and on-premises email servers using a variety of different protocols. These efforts are almost certainly still ongoing.

This campaign has already targeted hundreds of U.S. and foreign organizations worldwide, including U.S. government and Department of Defense entities. While the sum of the targeting is global in nature, the capability has predominantly focused on entities in the United States and Europe.

# Infoblox Threat Reports and Cyber Threat Alerts – Q3 2021

## Reply-Chain Threadjacking Campaign Delivers Squirrelwaffle Loader and Cobalt Strike

On September 13, security researchers discovered a malicious phishing campaign that uses reply-chain threadjacking to distribute a downloader known as Squirrelwaffle: an emerging threat that is delivered on the TR botnet and has the same infrastructure as that of the QakBot banking trojan.

Squirrelwaffle downloads the commercial penetration-testing product Cobalt Strike and uses it to deploy Beacon: a program that lets attackers carry out command execution, key logging, file transfer, privilege escalation, port scanning, lateral movement and other post-exploitation functions.

Read the Full Report →

## Likely FIN7 Recon Campaign

Since late August, Infoblox has been tracking a campaign distributing JavaScript malware. The command and control (C&C) domain, distribution method, and code used by these actors are consistent with those used by FIN7: a group of Russian cyber criminals who are motivated by financial gain and who have been targeting businesses around the world since 2013.

This group is focused on U.S. companies and English-speaking individuals, and it is known for its aggressiveness, creative use of social media, blackmailing, and threats to disclose victims' personal data.

The behavior of the malware in this campaign matched that of Griffon: a JavaScript malware attributed to FIN7. The behavior was also consistent with the assessment that this malware was being used as a first-stage reconnaissance tool and as an installer for future payloads.

Read the Full Report →

## Fake Delivery Emails Deliver AsyncRAT

On September 24, Infoblox observed a malicious email campaign distributing the remote access trojan (RAT) AsyncRAT, which has also been used in cyber attacks on the aviation industry. AsyncRAT is being propagated via a weaponized executable attached to emails made to appear to be coming from DHL.

AsyncRAT, also known as RevengeRAT, is designed to remotely monitor and control an infected computer through a secure, encrypted connection. It can be dropped by other malware, downloaded, or received as an email attachment.

Read the Full Report →

## XpertRAT Returns

From September 9 to 16, Infoblox observed a malspam campaign whose actors were impersonating an employee of the Dubai-based engineering and construction company Arar Infra Contracting LLC. The body of the malspam email attempted to lure its targets into opening an attached file that contained XpertRAT: a remote access trojan that has been around since 2011.

XpertRAT consists of a core component and multiple modules, all written in Delphi. Its remote access capability makes it popular among many cyber criminals. It is usually propagated via spam emails, but pirated media and fraudulent updates have also been used to propagate it.

Read the Full Report ➜

## Hancitor Adds Second Redirect

On September 8, Infoblox observed a malspam campaign that used DocuSign-themed lures to entice users to download and open Microsoft Word documents with malicious macros that installed embedded copies of the trojan downloader Hancitor.

We have written about previous Hancitor campaigns in April 2020, December 2020, March 2021, and June 2021. Hancitor's core characteristics have not changed, but in this campaign, Hancitor has yet another URL-redirection stage that precedes the delivery of the malicious document payload.

Read the Full Report ➜

## GuLoader Delivers Remcos RAT

On September 1 and 2, Infoblox observed a malicious email campaign distributing the trojan downloader GuLoader. The malware downloaded and executed the remote access trojan (RAT) Remcos. Although this campaign used GuLoader to deliver Remcos, other campaigns have used GuLoader to drop other kinds of RATs, such as NanoCore.

Security researchers first discovered GuLoader in December 2019. The malware, written in Visual Basic 6.0, is primarily used to download RATs and information stealers.

As a typical RAT, Remcos can steal information by capturing keystrokes, taking screenshots, checking browser caches and settings, and searching for files that contain passwords.

Read the Full Report ➜

## New Malware: Capturador Hijacker

Since September 1, we have been tracking a malspam campaign distributing malware that we had not observed yet and that has not been publicly reported on in the industry. The malware is a hijacker that we named Capturador, and we believe that the campaign has been targeting speakers of Portuguese as well as small and medium-size Brazilian companies. The campaign's emails contain RAR archives as attachments and, in the subject lines, contain references to budget requests and incoming invoices.

Read the Full Report ➜

## Hive Ransomware

On August 25, the FBI released a flash alert that described the Hive ransomware and related indicators of compromise (IOCs). According to the flash alert, Hive was discovered in June 2021 and likely operates as an affiliate-based ransomware. It uses common ransomware TTPs to compromise victims' machines, bypass anti-malware systems, and then steal sensitive data and encrypt system files. In addition, Hive leaves an unencrypted, plain-text note that threatens to leak the victim's data on the TOR website HiveLeaks unless the victim pays a ransom. This behavior is consistent with the recent trend wherein many ransomware campaigns attempt to extort victims and most exfiltrate data.

Read the Full Report ➜

## Fake Shipping Emails Deliver Ratty RAT

On August 8, Infoblox observed a malicious email campaign distributing the remote access trojan (RAT) Ratty via weaponized Java files. Emails in this campaign appeared to be coming from DHL and contained text that looked like shipping instructions.

Ratty is an open-source Java RAT. It was made available on GitHub and was strongly endorsed on hack forums. Although Ratty's original uploaders deleted the repository sometime in 2017, clones of Ratty exist.

Read the Full Report ➜

## OnePercent Group Ransomware Campaign

On August 23, the FBI released a flash alert about an ongoing campaign conducted by the OnePercent Group, which has been using Cobalt Strike to launch ransomware attacks against U.S. companies since November 2020. The alert also provided a list of IOCs associated with the campaign.

Read the Full Report ➜

## “Urgent Report” Spam Drops Danabot Banking Trojan

On August 12, Infoblox observed a malspam campaign distributing the banking trojan Danabot through ZIP files. This trojan was first seen by Proofpoint in 2018, is written in Delphi, and is capable of stealing credentials, taking screenshots, logging keystrokes, exfiltrating data to command and control (C&C) servers, and performing web injection to manipulate browser sessions and steal banking information.

Read the Full Report →

## Update on the Attack on the Italian Regional Data Center

On August 1, the regional data center of Lazio, the Italian region that includes Rome, was targeted by a cyber attack. The data center, known as Centro di Elaborazione Dati (CED), hosts several critical services: the portal where Lazio residents register for vaccination, and the portal where Lazio residents book medical examinations. Italian authorities had to shut down CED, and this slowed down the vaccination process. After delivering a ransomware, the attackers encrypted most of the CED files.

The FBI and Interpol joined forces with the Polizia Postale, the Italian police unit that specializes in cyber crime, to look for possible correlations between the ransomware used in the CED attack and the ransomware used in recent similar attacks against industrial targets and institutions around the world.

Read the Full Report →

## Transfer-Themed Malspam Drops STRRAT

On August 11, Infoblox observed an email campaign distributing the STRRAT trojan via weaponized file attachments. STRRAT is a Java-based remote access trojan (RAT) that is delivered in malicious email campaigns. Although Java runs on all operating systems, STRRAT is compatible only with Windows hosts. STRRAT can exfiltrate passwords to a command and control (C&C) server, run code on infected hosts, enable attackers to control infected hosts directly, and create reverse proxies. In addition, it has a rudimentary ransomware module.

Read the Full Report →

## New Spam Actor: EggshellCheetah

EggshellCheetah is the actor behind the high-volume spam campaigns that send emails with links to sites that pose as legitimate. EggshellCheetah aims to collect financial information, sell counterfeit products, and disseminate malspam supporting other actors’ scams. The campaigns employ a variety of lure topics, many of which have political themes.

Read the Full Report →

## Swift Payment-Themed Malspam Delivers Oski Stealer

On August 3, Infoblox observed a malicious malspam campaign distributing Oski Stealer, which is best known as a credential stealer. According to Cisco Talos, Oski Stealer shares code (thus traits) with Vidar and Arkei Stealer.

Read the Full Report →

## LemonDuck Trojan Delivers Cryptominers and Other Malware

On July 29, Microsoft reported a series of ongoing malware campaigns that involve LemonDuck: a trojan botnet that installs cryptominers and other malware. The majority of LemonDuck's targets are businesses in the manufacturing and IoT industries, and it has been seen across the world, including the United States, Russia, China, Germany, and the United Kingdom. LemonDuck is one of the few known botnets that target Linux as well as Windows systems, and its capabilities have been expanding rapidly in recent months.

Read the Full Report →

## Cyber Threat Advisory: Attack on Italian Regional Data Center

On August 1, the COVID-19 Crisis Unit for the Lazio region of Italy, which includes Rome, announced that a powerful cyber attack was targeting the regional data center, known as Centro di Elaborazione Dati (CED). The attack started after 00:00 CEST and lasted until at least 14:00 CEST. The attack forced the Italian authorities to shut down the CED, which is hosting, among other services, the portal where all Lazio residents register for vaccination. According to Alessio D'Amato, the head of the Regional Health Service of Lazio, the attack halted the registration process, and this probably slowed down the vaccination process. The authorities also shut down the Centro Unico di Prenotazione: the platform where all Lazio residents book medical examinations.

Read the Full Report →

## Infoblox Identifies New Threat Actor: WhiteSawShark and New Malware, HadLoader

In December 2020, the Infoblox Cyber Intelligence Unit discovered a spam actor we call WhiteSawShark. This actor targets a wide audience through campaigns that deliver Agent Tesla, FormBook, Loki, Remcos, Snake, and other infostealers and remote access trojans. The actor also uses a custom downloader, which we designated HadLoader.

We discovered WhiteSawShark by tracking spam campaigns sent from a set of recurring similar domains. Through analysis of the malware distributed from this infrastructure, we uncovered 16 additional domains, which serve as C&C servers and spam distribution servers.

Our analysis revealed that WhiteSawShark sent two types of malicious attachments: rich text format (RTF) documents that exploit vulnerability CVE-2017-11882, and archives that contain the final payload in compressed form. All the malware families that we saw WhiteSawShark distribute are available as malware-as-a-service (MaaS).

Read the Full Report ➔

## Purchase Order Malspam Delivers Snake Keylogger

On July 22, Infoblox found a malspam campaign distributing Snake Keylogger. The attachments in the emails of this campaign are rich text format (RTF) files that contain an exploit of CVE-2017-11882, a well-known vulnerability in Microsoft Office Equation Editor. Snake Keylogger's code has many similarities with other keyloggers, such as Phoenix, 404, Cheetah, and Matiex. It is likely that these five keyloggers are derived from the same codebase.

First discovered in November 2020, Snake Keylogger is a modular .NET infostealer. Threat actors use the malware's builder to define and configure specific features when generating new payloads. Snake Keylogger steals credential and configuration information by parsing login data from web browser databases, email clients, Wi-Fi network configuration files, and chat clients. It can also log keyboard strokes, take screenshots, and extract information from the system clipboard.

Read the Full Report ➔

## Cyber Threat Advisory: APT31 Targeting France

On July 21, the National Cybersecurity Agency of France published an advisory on Chinese Advanced Persistent Threat APT31, which was first identified in 2016 and is also known as Zirconium, Judgment Panda, and Bronze Vinewood. The advisory provided IP addresses of known compromised devices.

Germany's Federal Office for the Protection of the Constitution (BfV) reported on APT31 activities earlier this year. The U.S. government has also been reporting on cyber-espionage activity attributed to China: on July 19, the FBI and the Cybersecurity and Infrastructure Security Agency (CISA) reported on activity by APT40, another Chinese state–sponsored threat group.

In the past, APT31 has targeted the Parliament of Finland and companies involved in defense and security industries.

Read the Full Report →

## Adult-Themed Mimail Worm Campaign Steals Victim Information

On July 13, Infoblox observed a malicious email campaign that has been distributing the Mimail worm via weaponized executable files. Emails in this campaign try to lure victims into opening attachments that appear to be images of sexual nature. Mimail emerged in August of 2003, has spawned many variants, and is used to steal financial and sensitive data. Mimail variants contain payloads that can steal credit card information and credentials from web browsers and via a fake license expiry form. As a mass mailing worm, it propagates by distributing itself to victims' email contacts.

When we analyzed the malware, we found not only a warning against filtering out the emails but also a threat to DoS-attack targets that refused to heed that warning. However, we did not find this variant of the malware to have the capability to carry out the threat.

Read the Full Report →

## Cyber Threat Advisory: U.S. Oil Pipeline Intrusion

On July 20, the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI published joint advisory AA21-201A on a Chinese state–sponsored spear-phishing and intrusion campaign that targeted U.S. oil and natural gas pipeline companies from 2011 to 2013. The advisory identified a number of U.S. natural gas pipeline operators that were targeted during that time; out of those, 13 were confirmed compromised, 3 were not impacted, and 8 experienced an intrusion of unknown depth.

Based on the data that the actors stole and the tactics, techniques, and procedures (TTPs) used in the campaign, CISA and FBI assessed that the purpose of the intrusions was not only to steal intellectual property but also to gain strategic access to the industrial control system (ICS) networks and to prepare for future operations. The advisory provides information on the TTPs and lists the IOCs related to the campaign.

Read the Full Report →

## Cyber Threat Advisory: APT40 TTPs and Trends

On July 19, the FBI and CISA published a joint advisory on a Chinese advanced persistent threat APT40, also known as Bronze Mohawk, Feverdream, and Mudcarp. The advisory provided information about the APT's tactics, TTPs, IOCs and mitigation recommendations.

On this same day, the FBI, CISA, and NSA published a joint advisory on trends in cyber-espionage activity that they observed across various Chinese state–sponsored actors. These advisories coincided with the White House's July statement accusing the People's Republic of China (PRC) of hiring malicious actors to conduct, in early March 2021, cyber-espionage operations that exploited zero-day vulnerabilities in Microsoft Exchange Servers.

Read the Full Report ➔

## Spoofed Kazakh Malspam Delivers Neshta Infostealer

From March 5 to 15, Infoblox observed a malspam campaign distributing Neshta malware. Neshta is a computer virus that steals sensitive data by injecting malicious code into target executable files. Neshta is also capable of downloading other malware. First observed in 2003 and previously associated with BlackPOS malware, Neshta is still prevalent in the wild.

The threat actors behind this variant of Neshta exploited CVE-2017-11882, an old Microsoft Office memory corruption vulnerability, which enabled them to deliver the malware via email, web and USB devices.

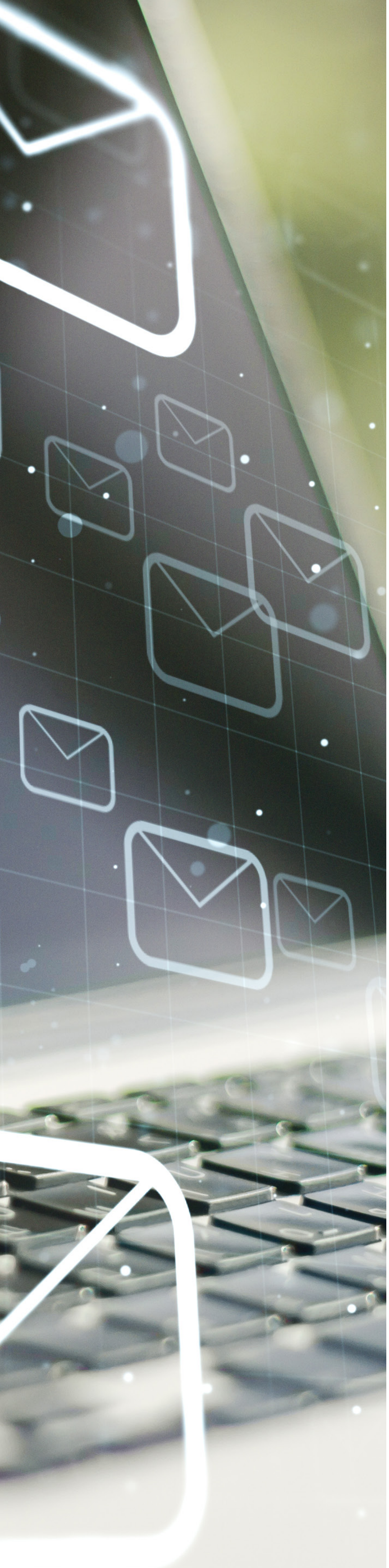
Read the Full Report ➔

## Cyber Threat Advisory: SonicWall Vulnerability

On July 15, the CISA issued an alert about threat actors actively targeting a known and previously patched vulnerability in SonicWall's secure mobile access (SMA) 100 series and secure remote access (SRA) products that run on unpatched and end-of-life (EOL) 8.x firmware.

On July 15, SonicWall confirmed CISA's alert about the vulnerability being actively exploited in the wild and urged its customers to take steps to reduce the risk of getting attacked. SonicWall has already identified three vulnerabilities that affect SRA 4600 and SMA 100 devices: CVE-2019-7481, CVE-2019-7482 and CVE-2021-20016.

Read the Full Report ➔



## Fake Kaseya Patch Malspam Campaign

On July 6, we observed a malspam campaign that was distributing an executable file containing Cobalt Strike: a legitimate, commercially available penetration-testing tool frequently abused by threat actors. Taking advantage of the recent ransomware attack on users of Kaseya's remote monitoring and management service VSA, the campaign attempted to get its targets to download and run a file that it claimed was the update meant to patch a recently exploited vulnerability in VSA.

We have previously reported on the ransomware attack on Kaseya's VSA, and we have observed additional emails and malicious files.

Read the Full Report →

## Cyber Threat Advisory: Kaseya Ransomware Attack Update: Patch Available

On July 2, the REvil ransomware group launched a supply chain attack that compromised Kaseya's VSA, a remote monitoring and management software platform, to hit a large number of managed service providers (MSPs). REvil used a fake update that exploited a zero-day vulnerability to deliver the ransomware and encrypt many machines.

On July 8, Infoblox released a Cyber Threat Advisory report that discussed the background of REvil, also known as Sodinokibi, and the ransomware attack on Kaseya.

On July 11, Kaseya released a patch for its on-premises version of VSA, deployed the patch to its VSA SaaS offering, and started assisting its customers with deploying the patch.

On July 12, Kaseya confirmed that it had restored its VSA SaaS offerings.

Read the Full Report →

## Cyber Threat Advisory: DarkSide Ransomware Variant

On July 8, the CISA published a Malware Analysis Report (AR21-189A) on a variant of the DarkSide ransomware. To date, there is no evidence that the variant has any association with the Colonial Pipeline security breach, which happened on May 7 and about which Infoblox released a CTA on May 13. This CTA summarized the information from CISA on DarkSide's new variant: a 32-bit dynamic-link library (DLL) named *encryptor2[.]dll*. This variant can delete Microsoft Volume Shadow copies, collect and encrypt files, and exfiltrate system information to its command and control (C&C) server. After encrypting the files, the program creates a bitmap image and sets it as the user's wallpaper. In the wallpaper, the program stores the details that the victim would need to recover data.

Read the Full Report →

## Malspam RTF Files Drop Formbook Infostealer

On July 2, Infoblox observed a malicious email campaign that was distributing Formbook malware via weaponized rich text format (RTF) files. Emails in this campaign came from someone who appeared to be interested in purchasing goods that the recipient might be selling.

Infoblox has reported on Formbook campaigns several times in the past. To lure victims into opening malicious attachments, the campaigns usually leverage financial themes, coronavirus-related messaging and other current topics.

Formbook is a well-known infostealer and form-grabber malware, and it is sold as malware-as-a-service (MaaS) in underground forums. It can communicate with command and control (C&C) servers, and it has evasion capabilities, such as process hollowing, webform hijacking, keylogging and clipboard monitoring.

Read the Full Report ➜

## Cyber Threat Advisory: Kaseya REvil Ransomware Attack

On July 2, the threat actors behind REvil, also known as Sodinokibi, launched a massive ransomware 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 was 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 a universal decryptor—our price is 70,000,000$ in BTC and we will publish a decryptor that decrypts files of all victims, so everyone will be able to recover from attack in less than an hour."

Read the Full Report ➜

## Fancy Bear Brute Force Attacks

On July 1, the NSA, CISA, FBI, and NCSC published a joint advisory on a brute-force campaign that leveraged a Kubernetes cluster to attack government and private organizations around the world. The advisory attributed the campaign to the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), but private cybersecurity companies have also referred to the actor as Fancy Bear, APT28 or Strontium.

The advisory described the campaign as "almost certainly still ongoing" and targeting mainly users of Microsoft Office 365 Cloud services. The campaign has been most active in the United States and Europe, and its main targets are government and military organizations, political parties, defense contractors, energy companies, law firms and higher-education institutions.

Read the Full Report ➜

# 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