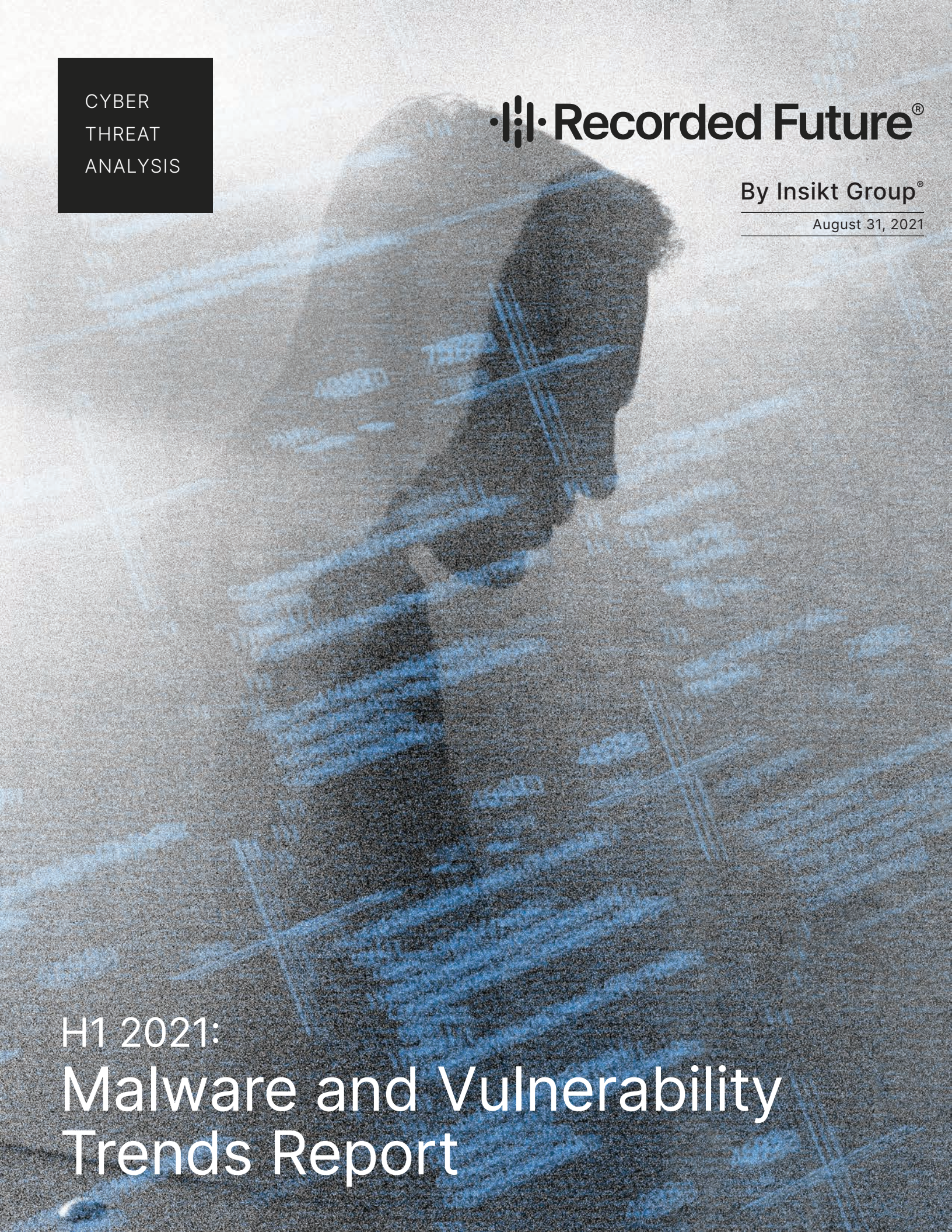
CYBER
THREAT
ANALYSIS

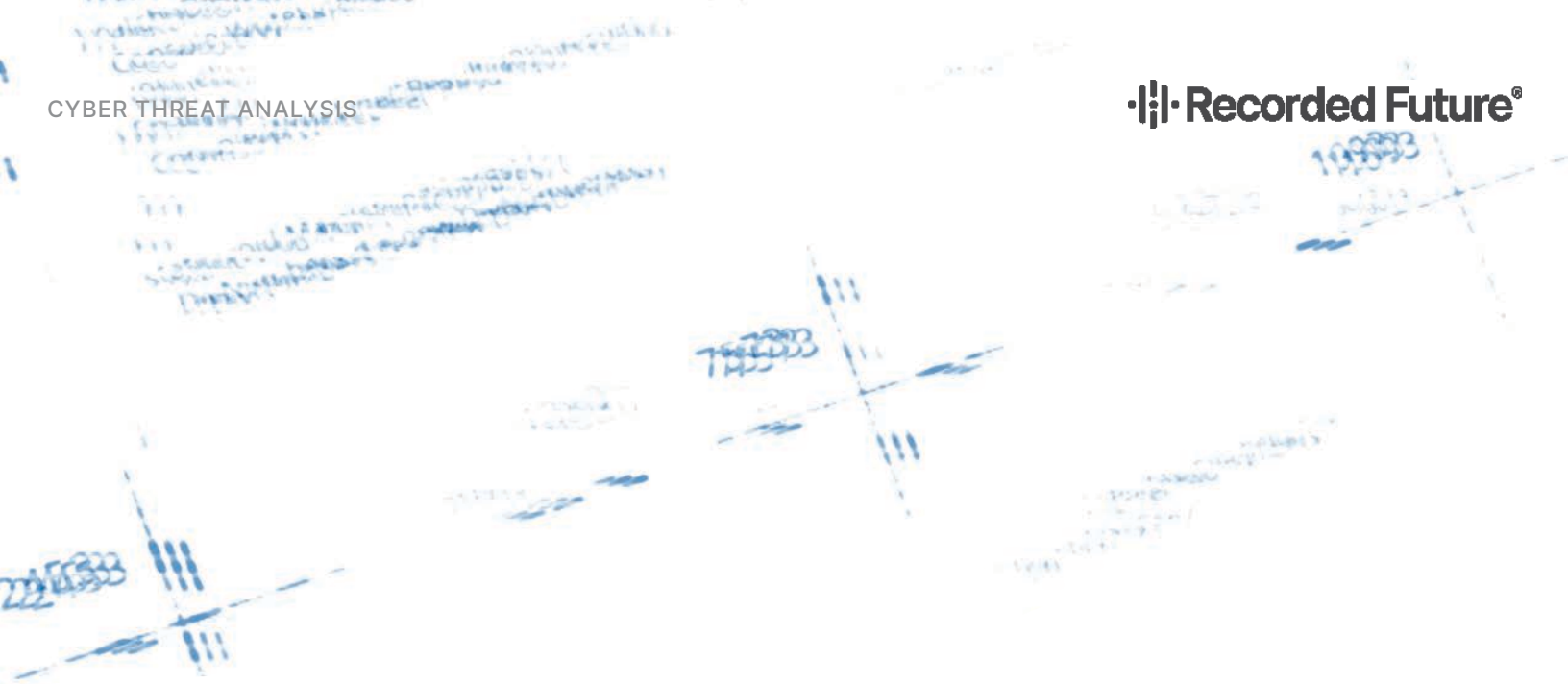
Recorded Future®

By Insikt Group®

August 31, 2021



H1 2021: Malware and Vulnerability Trends Report



This report examines trends in malware use, distribution, and development, and high-risk vulnerabilities disclosed by major hardware and software vendors between January 1 and June 30, 2021. Data was assembled from the Recorded Future® Platform, open-source intelligence (OSINT), and public reporting on NVD data. This report will assist threat hunters and security operations center (SOC) teams in strengthening their security posture by prioritizing hunting techniques and detection methods based on this research and data along with vulnerability teams looking for ways to prioritize patching and identify trends in vulnerability targeting.

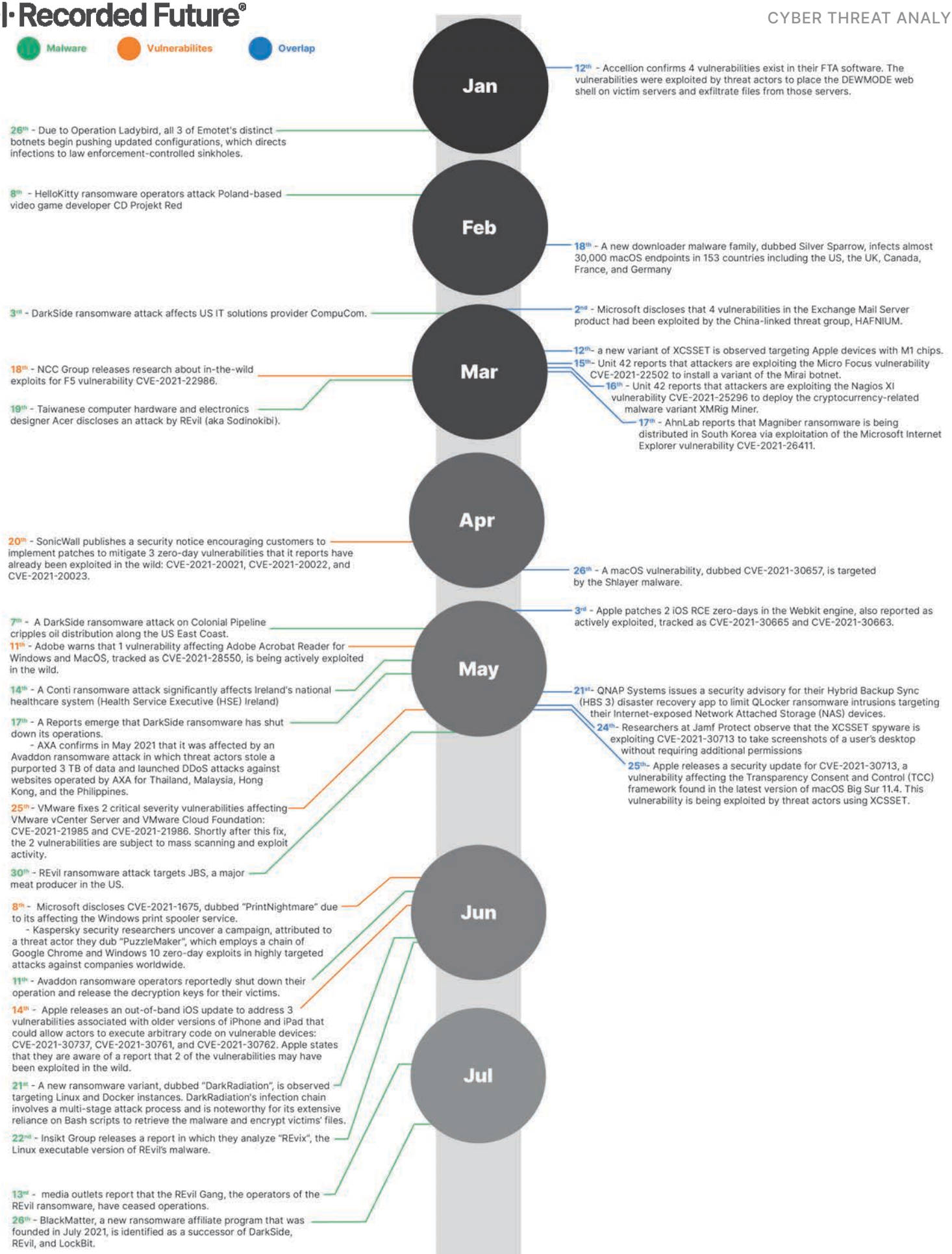
Executive Summary

Trends within vulnerability exploitation and malware attacks often intersect, as threat groups will target these flaws to deliver, distribute, and execute their malicious code onto vulnerable systems. Throughout the first half of 2021, several notable cyber incidents gained mainstream attention due to their wide effect and novel techniques used in attacks that demonstrate this intersection. These incidents involved threat actors taking advantage of critical vulnerabilities to deploy malware onto compromised systems such as Accellion FTA software, Microsoft Exchange Servers, macOS, and QNAP devices. These attacks illustrate the rapid targeting and exploitation of high-risk vulnerabilities by cybercriminals, ransomware operators, and state-sponsored groups alike.

In the first half of 2021, the marketplace for ransomware matured as more operators began hiring affiliates to increase the effectiveness of their attacks. Ransomware operators have demonstrated increased sophistication by adding DDoS to their attacks, targeting Linux systems, rapidly exploiting newly disclosed vulnerabilities, and even targeting zero-day vulnerabilities in attacks. This evolution demonstrates that ransomware operators are no longer considered unorganized cybercriminals, but now have the resources to compete with well-established groups like nation-state threat actors.

In an investigation into botnet activity, the successful law enforcement takedown of the Emotet botnet in January 2021 opened a gap in the botnet space, resulting in the increased use of other bots, including Trickbot, IcedID, BazarLoader, and Qakbot over the last quarter.

For trends within the vulnerability landscape in H1 2021, supply-chain attacks derived from vulnerabilities in third-party products dominated headlines. In addition, vulnerabilities in corporate software were more frequently targeted than consumer-grade software, and high-risk vulnerabilities across major vendors spiked in the first half of the year.


Malware
Vulnerabilites
Overlap
Jan
12th - Accellion confirms 4 vulnerabilities exist in their FTA software. The vulnerabilities were exploited by threat actors to place the DEWMODE web shell on victim servers and exfiltrate files from those servers.
26th - Due to Operation Ladybird, all 3 of Emotet's distinct botnets begin pushing updated configurations, which directs infections to law enforcement-controlled sinkholes.
Feb
8th - HelloKitty ransomware operators attack Poland-based video game developer CD Projekt Red
18th - A new downloader malware family, dubbed Silver Sparrow, infects almost 30,000 macOS endpoints in 153 countries including the US, the UK, Canada, France, and Germany
Mar
3rd - DarkSide ransomware attack affects US IT solutions provider CompuCom.
2nd - Microsoft discloses that 4 vulnerabilities in the Exchange Mail Server product had been exploited by the China-linked threat group, HAFNIUM.
12th- a new variant of XCSSET is observed targeting Apple devices with M1 chips.
15th- Unit 42 reports that attackers are exploiting the Micro Focus vulnerability CVE-2021-22502 to install a variant of the Mirai botnet.
16th - Unit 42 reports that attackers are exploiting the Nagios XI vulnerability CVE-2021-25296 to deploy the cryptocurrency-related malware variant XMRig Miner.
17th - AhnLab reports that Magniber ransomware is being distributed in South Korea via exploitation of the Microsoft Internet Explorer vulnerability CVE-2021-26411.
18th - NCC Group releases research about in-the-wild exploits for F5 vulnerability CVE-2021-22986.
19th - Taiwanese computer hardware and electronics designer Acer discloses an attack by REvil (aka Sodinokibi).
Apr
20th - SonicWall publishes a security notice encouraging customers to implement patches to mitigate 3 zero-day vulnerabilities that it reports have already been exploited in the wild: CVE-2021-20021, CVE-2021-20022, and CVE-2021-20023.
26th - A macOS vulnerability, dubbed CVE-2021-30657, is targeted by the Shlayer malware.
May
3rd - Apple patches 2 iOS RCE zero-days in the Webkit engine, also reported as actively exploited, tracked as CVE-2021-30665 and CVE-2021-30663.
7th - A DarkSide ransomware attack on Colonial Pipeline cripples oil distribution along the US East Coast.
11th - Adobe warns that 1 vulnerability affecting Adobe Acrobat Reader for Windows and MacOS, tracked as CVE-2021-28550, is being actively exploited in the wild.
14th - A Conti ransomware attack significantly affects Ireland's national healthcare system (Health Service Executive (HSE) Ireland)
17th - A Reports emerge that DarkSide ransomware has shut down its operations.
- AXA confirms in May 2021 that it was affected by an Avaddon ransomware attack in which threat actors stole a purported 3 TB of data and launched DDoS attacks against websites operated by AXA for Thailand, Malaysia, Hong Kong, and the Philippines.
21st- QNAP Systems issues a security advisory for their Hybrid Backup Sync (HBS 3) disaster recovery app to limit QLocker ransomware intrusions targeting their Internet-exposed Network Attached Storage (NAS) devices.
24th- Researchers at Jamf Protect observe that the XCSSET spyware is exploiting CVE-2021-30713 to take screenshots of a user's desktop without requiring additional permissions
25th- Apple releases a security update for CVE-2021-30713, a vulnerability affecting the Transparency Consent and Control (TCC) framework found in the latest version of macOS Big Sur 11.4. This vulnerability is being exploited by threat actors using XCSSET.
25th- VMware fixes 2 critical severity vulnerabilities affecting VMware vCenter Server and VMware Cloud Foundation: CVE-2021-21985 and CVE-2021-21986. Shortly after this fix, the 2 vulnerabilities are subject to mass scanning and exploit activity.
30th - REvil ransomware attack targets JBS, a major meat producer in the US.
Jun
8th - Microsoft discloses CVE-2021-1675, dubbed "PrintNightmare" due to its affecting the Windows print spooler service.
- Kaspersky security researchers uncover a campaign, attributed to a threat actor they dub "PuzzleMaker", which employs a chain of Google Chrome and Windows 10 zero-day exploits in highly targeted attacks against companies worldwide.
11th - Avaddon ransomware operators reportedly shut down their operation and release the decryption keys for their victims.
14th - Apple releases an out-of-band iOS update to address 3 vulnerabilities associated with older versions of iPhone and iPad that could allow actors to execute arbitrary code on vulnerable devices: CVE-2021-30737, CVE-2021-30761, and CVE-2021-30762. Apple states that they are aware of a report that 2 of the vulnerabilities may have been exploited in the wild.
Jul
21st - A new ransomware variant, dubbed "DarkRadiation", is observed targeting Linux and Docker instances. DarkRadiation's infection chain involves a multi-stage attack process and is noteworthy for its extensive reliance on Bash scripts to retrieve the malware and encrypt victims' files.
22nd - Insikt Group releases a report in which they analyze "REvix", the Linux executable version of REvil's malware.
13rd - media outlets report that the REvil Gang, the operators of the REvil ransomware, have ceased operations.
26th - BlackMatter, a new ransomware affiliate program that was founded in July 2021, is identified as a successor of DarkSide, REvil, and LockBit.

Section I — Shared Malware and Vulnerability Trends and Events

Throughout the first half of 2021, several cyber incidents involving threat actors taking advantage of critical vulnerabilities to deploy malware onto compromised systems gained mainstream attention. Attacks on Accellion FTA software, Microsoft Exchange Servers, macOS, and QNAP devices demonstrated the rapid exploitation of high-value vulnerabilities by cybercriminals, ransomware operators, and state-sponsored groups alike.

Malware Exploits Accellion FTA Vulnerabilities

In January 2021, Accellion confirmed the existence of vulnerabilities in its legacy FTA software. They further claimed that they first learned of the vulnerability in mid-December 2020 and that a patch was subsequently released "in 72 hours with minimal impact". However, within a few weeks after Accellion's initial press release, multiple other companies disclosed data breaches that occurred due to the exploitation of Accellion FTA. Data from victims of the Accellion FTA compromise began to appear on the website CL0P LEAKS, indicating that Clop ransomware took advantage of unpatched vulnerabilities CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104.

In addition, these vulnerabilities in the FTA software were exploited by threat actors to place the DEWMODE web shell on victim servers and exfiltrate files from those servers, with initial access gained through an SQL injection vulnerability, CVE-2021-27101. The threat actor's exploitation of zero-day vulnerabilities in Accellion FTA was key to gaining access to these servers and further exploiting them.

Microsoft Exchange Server Vulnerabilities Actively Targeted

In March 2021, Microsoft disclosed that 4 vulnerabilities in the Exchange Mail Server product were being actively exploited, with servers from 2013 onwards (2016, 2019) vulnerable; Microsoft released patches for the vulnerabilities the same day. The exploits were tied to HAFNIUM, a China-linked espionage threat group targeting scientists, think tanks, private legal entities, and defense contractors. The exploited vulnerabilities are collectively called ProxyLogon and are tracked as CVE-2021-26855, CVE-2021-27065, CVE-2021-26857, and CVE-2021-26858.

According to Microsoft, researchers found that many of the compromised systems had multiple web shells within their environment. Throughout March 2021, CISA identified 9 web shells associated with Exchange Server targeting. CISA identified them as China Chopper web shells, which have been identified in the wild since at least 2013 and are a tool attackers can use post-exploitation, allowing them to execute code remotely on the compromised servers. China Chopper is an Active Server Page Extended (ASPX) web shell that is very small compared to other exploits and contains a web shell command-and-control (C2) client binary and a text-based web shell payload. CISA provided YARA rules and mitigation recommendations within their alert.

Malware Targeting MacOS

While vulnerabilities and malware affecting Windows and networking devices took center stage in the first half of 2021, there were reports of 2 malware variants exploiting macOS vulnerabilities, Shlayer and XCSSET, and 1 adware variant, SliverSparrow, uniquely using JavaScript for execution on macOS devices.

In May 2021, Apple released a security update for CVE-2021-30713, a vulnerability affecting the Transparency Consent and Control (TCC) framework found in the latest version of macOS Big Sur 11.4. This vulnerability was being exploited by threat actors using XCSSET. Trend Micro security researchers first discovered XCSSET in August 2020, but in March 2021, a new variant of XCSSET was observed targeting Apple devices with M1 chips. In May 2021, researchers at Jamf Protect observed the XCSSET spyware exploiting CVE-2021-30713 to take screenshots of a user's desktop without requiring additional permissions. Jamf researchers also stated that XCSSET also abuses CVE-2021-30713 to hijack other permissions beyond taking screenshots.

Also in May 2021, Apple patched 2 iOS RCE zero-days in the Webkit engine, also reported as actively exploited, tracked as CVE-2021-30665 and CVE-2021-30663. In April 2021, a separate macOS vulnerability tracked as CVE-2021-30657 was targeted by the Shlayer malware, with Kaspersky stating in a January 2020 report that Shlayer accounted for almost 30% of malware detections for macOS.

In mid-February 2021, security operations firm Red Canary reported on a new downloader malware family, dubbed Silver Sparrow, that had infected almost 30,000 macOS endpoints in 153 countries including the US, the UK, Canada, France, and Germany using JavaScript for execution on macOS devices in a novel way. According to Red Canary, what makes the malware unique is that its installer packages use the macOS Installer JavaScript API to execute commands. While this is common for legitimate software, it is very uncommon for macOS installers, which usually use pre-install or post-install scripts to execute commands.

QLocker Ransomware Exploits QNAP Devices

On May 21, 2021, QNAP Systems Inc. issued an advisory that advised its customers to update their Hybrid Backup Sync (HBS 3) disaster recovery app to limit QLocker ransomware intrusions targeting their internet-exposed network-attached storage (NAS) devices. The company noted that the ransomware campaign started on the week of April 19, 2021, in which QLocker ransomware operators exploited CVE-2021-28799 to target QNAP NAS running specific versions of HBS 3 (Hybrid Backup Sync). The vulnerability acted as a backdoor account, enabling attackers to access devices running out-of-date HBS 3 versions. Additionally, QNAP believes that the threat actors are exploiting 2 other vulnerabilities in its products: CVE-2020-2509 and CVE-2020-36195.

Section II — Malware Roundup

In the first half of 2021, ransomware and botnets took center stage in the malware threat landscape. Ransomware operators updated their TTPs by adding DDoS to their threats and targeting Linux systems, and they experienced government disruptions and ostracization on dark web forums after targeting critical infrastructure, which led to several prominent operations shutting down.

In an investigation into botnet activity, the successful law enforcement takedown of the Emotet botnet in January 2021 opened a gap in the botnet space, resulting in the increased use of other bots, including Trickbot, IcedID, BazarLoader, and Qakbot over the last quarter.

Ransomware Trends

Affiliate Programs and Initial Access Brokers Profit From Attacks

Ransomware attacks have proven to be a successful business model for cybercriminals in the last year, with operators making at least $350 million in ransom payments in 2020, according to a Chainalysis report. H1 2021 illustrated the evolution that the ransomware landscape took between 2019 and 2020 to 2021. In 2020, ransomware operators started acknowledging the value of extortion websites and affiliate programs. But in 2021, the overall marketplace for ransomware matured as more operators began hiring affiliates to increase the effectiveness of their attacks. In addition, ransomware operators often rely on compromised access from "initial access brokers", who advertise access to compromised networks.

Q1 2021 Ransomware Trends: Ransomware Targets Large Technology Companies

Q1 2021 was marked by ransomware attacks against large technology companies, notably the following 3, which garnered attention in the media: an attack most likely carried out by HelloKitty ransomware operators against Poland-based video game developer CD Projekt Red that occurred on February 8, 2021; a DarkSide ransomware attack that affected US IT solutions provider CompuCom disclosed on March 3, 2021; and an attack by REvil (aka Sodinokibi) operators against the Taiwanese computer hardware and electronics designer Acer, disclosed on March 19, 2021.

In the compromise of CompuCom, DarkSide ransomware operators used a Cobalt Strike Beacon installed in the company's environment to move laterally and steal administrative credentials that allowed them to deploy the ransomware payload on February 28, 2021.

Q2 2021 Ransomware Trends: Critical Infrastructure Targeting Followed by Ransomware Shutdowns

Ransomware gained significant media attention throughout Q2 2021, especially due to a DarkSide ransomware attack on Colonial Pipeline, a Conti ransomware attack on Ireland's national healthcare system (Health Service Executive (HSE) Ireland), global widespread Avaddon ransomware attacks, and a REvil ransomware attack on JBS. All of these attacks significantly disrupted services, and in the case of Colonial Pipeline, led to state emergencies and gas shortages across the US.

However, after these attacks gained attention from the media, Darkside ransomware, Avaddon, and REvil operators shutdown their operations. In mid-May 2021, reports emerged that DarkSide ransomware shutdown its operations. On June 11, 2021, Avaddon ransomware operators reportedly shutdown their operation and released the decryption keys for their victims, with Emsisoft releasing a free decrypter for Avaddon ransomware that all victims can use to recover their files. On July 13, 2021, media outlets [1, 2] reported that the REvil Gang, the operators of the REvil ransomware, ceased operations.

Following the REvil shutdown, BlackMatter, a new ransomware affiliate program founded in July 2021, succeeded DarkSide, REvil, and LockBit. According to their press release, "The project has incorporated in itself the best features of DarkSide, REvil, and LockBit". While these ransomware variants have reportedly ceased under their previous naming conventions, it is clear that some attributes persist through rebranding and updated features.

DDos Attacks Add to Ransomware Pain

Ransomware operators also increasingly added DDoS attacks to their campaigns. France-based insurance company AXA confirmed in May 2021 that it was affected by an Avaddon ransomware attack in which threat actors stole a purported 3 TB of data and launched DDoS attacks against websites operated by AXA for Thailand, Malaysia, Hong Kong, and the Philippines. News of this attack came shortly after warnings issued earlier in the month by the FBI and the Australian Cyber Security Centre (ACSC); both agencies had observed Avaddon ransomware attacks targeting organizations worldwide and across a wide array of industries. Though the Avaddon ransomware operation shutdown and released its decryption keys in June 2021, we expect ransomware operators to continue using this tactic. The overwhelming flood of web traffic created by DDoS attacks combined with file encryption and data theft put an enormous amount of pressure on victim organizations to pay the ransom to potentially avoid further downtime and data loss or leakage.

Ransomware Operators Shift to Linux Targets

Between June and July 2021, Recorded Future identified 3 ransomware operators who released ransomware variants targeting Linux systems. On June 21, 2021, a new ransomware variant, dubbed "DarkRadiation", was observed targeting Linux and Docker instances. DarkRadiation's infection chain involves a multi-stage attack process and is noteworthy for its extensive reliance on Bash scripts to retrieve the malware and encrypt victims' files. In addition, REvil now operates "REvix", a Linux-executable version of REvil's malware. While previously REvil targeted Windows systems with Sodinokibi, this is the first software from the group that targets Linux-based hypervisor infrastructure, affecting all the virtual (cloud) environments of the attacked organization. Lastly, Recorded Future has reported on a new Linux ransomware variant of BlackMatter ransomware.

Shift in Botnet landscape

The successful takedown of the Emotet botnet by law enforcement, dubbed Operation Ladybird, opened a gap in the botnet space, resulting in increased use of other bots, including Trickbot, IcedID, BazarLoader, and Qakbot, over the last quarter.

On January 27, 2021, a global team of law enforcement agencies announced the seizure and takedown of Emotet infrastructure and the arrest of an undisclosed number of operators. On January 26, 2021, all 3 of Emotet's distinct botnets began pushing updated configurations, which directed infections to law enforcement-controlled sinkholes. Following this update, previous Emotet Tier 1 servers stopped responding to normal probes and beacons because law enforcement seized hundreds of servers from Emotet's tiered infrastructure.

Despite frequent breaks, Emotet was one of the most prolific and profitable threats in 2019 and 2020. Since Operation Ladybird, several other malware families have continued to increase their activity into Q2 2021. Specifically, Trickbot, IcedID, BazarLoader, and Qakbot have established themselves as prominent botnets, with variants updating their downloader functions and delivery methods, becoming initial entry points used to deploy additional, more harmful malware, especially ransomware.

Section III — Vulnerability Roundup

The SolarWinds attack disclosed in December 2020 highlighted the significant risks posed by supply-chain vulnerabilities, and the threat landscape of compromise via a relationship with a vulnerable third-party continued to attract attention in Q1 2021 due to 2 major malicious campaigns. Coincidentally, in both cases, attackers reportedly exploited a set of 4 vulnerabilities in critical enterprise software to exfiltrate data from victim organizations. First were the attacks by the Clop ransomware operators against Accellion's file-sharing software FTA, which was affected by the vulnerabilities CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104. Second were the attacks against Microsoft Exchange Servers, first by the China-linked group HAFNIUM and then by many other APT groups, via exploitation of CVE-2021-26855 (ProxyLogon), CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065.

Enterprise Software Targeted More Than Consumer-Grade Software

These 2 campaigns were part of a trend in vulnerability exploitation for the first half of the year in which attackers ignored consumer-grade software in favor of technology normally used by business clients. In our report for the top 10 vulnerabilities of 2020 based on criminal interest, we found that many of the vulnerabilities that have been exploited for the last several years are associated with software used by the average information technology consumer, such as CVE-2017-11882 in Microsoft Office. However, in Q1 2021, the main trend in exploitation was of either business- or enterprise-class technology, such as Accellion FTA, Nagios XI, Microsoft Exchange, and F5 BIG-IP.

High-Risk Vulnerabilities Across Major Vendors Spiked in H1 2021

A trend that we identified at the end of 2020 and continued into Q1 2021 was a widening distribution of products affected by high-risk vulnerabilities. Microsoft products have historically been a major target of vulnerability exploitation; in early 2020, Microsoft dominated our list of high-risk vulnerabilities. However, in Q1 2021, Microsoft high-risk vulnerabilities accounted for less than 25% of the total 39. This contributed to the bottom line for Q2 2021: many critical vulnerabilities, affecting many vendors, many of which were exploited in the wild, which may have given some defenders the feeling that everything was on fire all the time. On any metric that matters to defenders (ease of exploit, distribution of vulnerabilities across a technology stack, severity of individual vulnerabilities, type of product affected, etc.), the high-risk vulnerabilities we identified presented major challenges to teams attempting to stay ahead of attacks against individual devices, corporate networks, and enterprise software. Critical, easily exploited vulnerabilities appeared in multiple products from prominent vendors such as Microsoft, Apple, Google, Adobe, Dell, SonicWall, QNAP, and VMWare. Moreover, in many cases these vulnerabilities had already been exploited by the time they were disclosed.

No single set of vulnerabilities earned as much coverage as the foursomes affecting either Accellion or Microsoft Exchange in Q1 2021, but Q2 2021 made up in quantity what it lacked in individual notoriety. The number of high-risk vulnerabilities in Recorded Future's data set spiked from 39 in Q1 to 70 in Q2 2021, and the number of vulnerabilities reported to be exploited jumped from 17 to 34. An issue for Microsoft users in the quarter was the disclosure of CVE-2021-1675, dubbed "PrintNightmare" due to its affecting the Windows print spooler service (a common service that was also famously exploited a decade ago by Stuxnet). The critical issue for PrintNightmare is that successful exploitation is not only relatively simple but can be done by a low-privileged account. This vulnerability was the most referenced for the quarter, in large part due to Microsoft's initially unsuccessful patching of the flaw, which is unusual for the company. As a result, the term "PrintNightmare" would come to include a second vulnerability, CVE-2021-34527, late in the quarter.

In Q2 2021, and for the first time since Q1 2020, Apple featured prominently among affected vendors. The exploitation of Apple software and devices aligns with a trend so far in 2021 of attackers targeting Apple products, such as the Silver Sparrow malware, which is the second known piece of macOS malware to feature a program compiled for the new M1 chip that Apple introduced in November 2020. In Q2 2021, attackers exploited vulnerabilities in Apple's MacOS, Safari, iPhone OS, iPad OS, tvOS, and WatchOS.

Section IV — Outlook

We expect ransomware to continue to be a significant threat and the number of new ransomware operators to increase as new threat groups adopt the effective business model of double extortion. Just 2 days into Q3 2021, IT management company Kaseya announced a REvil ransomware attack affecting users of their Virtual System Administrator (VSA) due to a zero-day vulnerability, CVE-2021-30116. The use of a zero-day by a ransomware operator is novel and demonstrates the evolution and development of the ransomware market.

In 2020, ransomware operators started acknowledging the value of extortion websites and affiliate programs. In 2021, the marketplace for ransomware matured as more operators began hiring affiliates to increase the effectiveness of their attacks. In addition, ransomware operators often rely on compromised access from "initial access brokers" who advertise access to compromised networks. These brokers allow operators to spread the workload across "contractors" or "affiliates", which increases their technical proficiency and the effectiveness of the attack. We expect the criminal underground market will continue to facilitate ransomware operations, potentially leading to an expansion in the market and an increase in demand for contractors due to the increasing number of ransomware operators and attacks. Therefore, we recommend security teams use Hunting Packages to proactively hunt for ransomware TTPs and signatures.

We expect botnet malware delivery to continue to increase, especially alongside the increase in ransomware, as these droppers are often used to facilitate ransomware attacks. It is critical to track and monitor these droppers, as this initial entry is the point in the attack kill chain where defenders can thwart an attack and significantly curtail business disruption.

As far as vulnerability prioritization, zero-day exploitation affecting Microsoft, Apple, and Google is naturally where most defenders will likely concentrate patching first, but H1 2021 featured malicious exploitation of vulnerabilities across many products and vendors. Facing this diversity, vulnerability management teams cannot take any piece of software or hardware for granted in their technology stack but instead need to confirm that they can quickly track everything in use in their stack, along with devices' or software's versions.

Finally, we anticipate that increased criminal targeting of Apple devices will continue, and that malware operators will use novel techniques and functionalities to exploit Apple devices. As a result, organizations that rely on iOS or MacOS should treat these systems as just as vulnerable as other prominent operating systems such as Windows or Android. We further recommend that system owners who are responsible for asset management and vulnerability management make sure their systems are not vulnerable or susceptible to known attacks.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.