LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Health Sector Cybersecurity: 2021 Retrospective and 2022 Look Ahead

03/03/2022

TLP: WHITE, ID# ***202203031300***

Agenda

- Introduction/Overview
- Healthcare Cybersecurity up to 2021
  - Timeline of Events and Incidents
- Healthcare Cybersecurity Throughout 2021
  - Detailed Timeline of Events and Incidents
- Healthcare Cybersecurity – 2022 and Beyond
  - How to Move Forward
- Conclusions
- References

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

- Cybercriminals and nation-states have engaged in cyberattacks against healthcare organizations for years
  - What is different about today?
  - What will we have to be concerned with tomorrow?
- In recent years and continuing today:
  - Ransomware continues to be relevant despite efforts to combat it
  - Data breaches are as common as ever
  - Vulnerabilities continue to be released; phishing and RDP continue to be compromised
- What's different about today?
  - Threat actors continue to evolve and become more sophisticated and effective
    - Distributed attack vectors are increasingly used
      - Managed service provider compromise
      - Supply chain compromise
      - Open-source software compromise
  - Governments are increasingly aggressive in fighting back
    - Despite this, healthcare organizations have as big a role as ever in defending themselves

1989 PC Cyborg “AIDS Trojan”

- The first ransomware attack occurred in 1989 and had a healthcare theme
  - Biologist Joseph Popp distributed 20,000 floppy disks at the World Health Organization AIDS conference in Stockholm in 1989.
  - The trojanized disks would install malicious code to track reboots, display ransom demand after 90 reboots on a victim system that would count reboots. After 90 reboots, the system would display a message claiming to be from 'PC Cyborg Corporation' which said their software lease had expired and that they needed to send $189 to an address in Panama to regain access to their system.
  - Popp was eventually charged with blackmail but was later declared mentally unfit to stand trial.

Timeline of Historic Healthcare Cybersecurity Events up to the Year 2021

Anonymous attacks Boston's Children's Hospital with distributed denial-of-service (DDoS) attacks.

APRIL 2014

Anthem Health Insurance attacked, with 80 million customer records accessed, including PII/PHI. China was likely the attacker.

FEBRUARY 2015

Hollywood Presbyterian Medical Center was attacked with ransomware and paid a then unheard-of ransom of $17,000 to recover their files.

FEBRUARY 2016

WannaCry exploits 200,000 systems across 150 countries, including 70,000 British NHS systems. Cost of the attack estimated to be £92 million.

MAY 2017

Timeline of Historic Healthcare Cybersecurity Events up to the Year 2021, Part 2

Brookside ENT and Hearing Center of Creek, MI announced it will close due to ransomware attack.

APRIL 2019

400 dental offices attacked with Ryuk ransomware via compromised managed service provider.

AUGUST 2019

Wood Ranch Medical in Simi Valley, CA announced it will close due to a ransomware attack.

SEPTEMBER 2019

Campbell County Health in Gillette, WY, was attacked with ransomware and canceled surgeries, transferred ER patients to alternative facilities and stopped accepting new patients.

SEPTEMBER 2019

Timeline of Historic Healthcare Cybersecurity Events up to the Year 2021, Part 3

DCH Health Systems of Alabama was attacked with Ryuk ransomware and was forced to stop admitting new non-critical patients.

OCTOBER 2019

Rouen University Hospital-Charles Nicolle in northern France attacked by ransomware that disabled 6,000 systems, hospital temporarily operated in "degraded mode".

NOVEMBER 2019

1.19 billion medical images discovered to have been leaked to the public over three months.

NOVEMBER 2019

Milwaukee, WI based Managed Service Virtual Care Provider attacked with Ryuk ransomware, 110 customer nursing homes temporarily lose access to resident health records.

NOVEMBER 2019

Timeline of Historic Healthcare Cybersecurity Events up to the Year 2021, Part 4

Cancer Center of Hawaii suffers ransomware attack and suspended cancer radiation services for a few days.

DECEMBER 2019

Hackensack Meridian Health of New Jersey was attacked with ransomware and was forced to cancel some surgical and other procedures.

DECEMBER 2019

Comparitech research on U.S. healthcare ransomware attacks observed 172 attacks on U.S. healthcare organizations since 2016 (costing over $157M)

FEBRUARY 2020

World Health Organization-themed phishing campaign dropping HawkEye malware (keylogger, credential stealer, dropper).

MARCH 2020

Timeline of Historic Healthcare Cybersecurity Events up to the Year 2021, Part 5

Despite promises to not target healthcare during the pandemic, Maze attacks Hammersmith Medicines Research prior to conducting coronavirus vaccine trials.

MARCH 2020

Barracuda Networks notes spike in covid-themed phishing attacks.

137 in January,
1,188 in February
9,116 in March

MARCH 2020

Google reports significant increase in phishing attacks since the Covid outbreak:

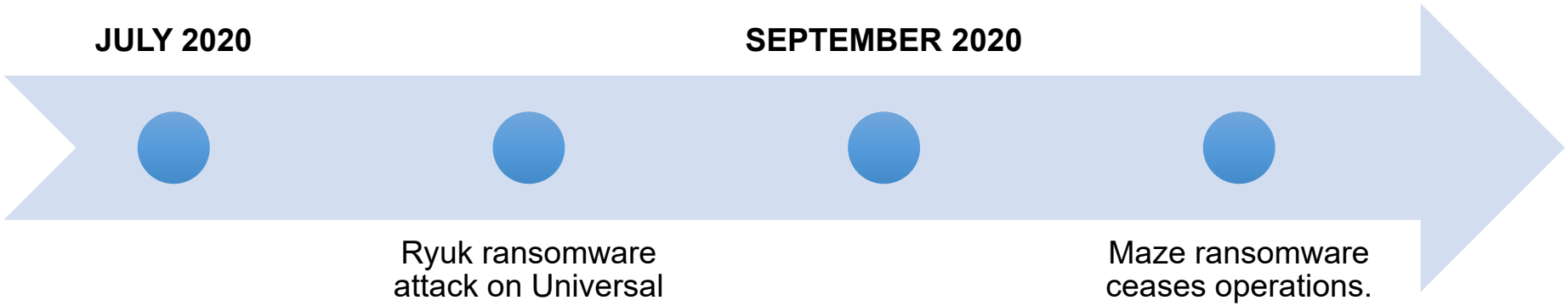
149,195 in January,
293,235 in February
522,495 in March

MARCH 2020

INTERPOL issues alert on an increase in cyberattacks, targeting organizations engaged in virus response.

APRIL 2020

Timeline of Historic Healthcare Cybersecurity Events up to the Year 2021, Part 6



McAfee report: Observed average of 375 covid-themed threats per minute in 2020 Q1.

JULY 2020

Ryuk ransomware attack on Universal Healthcare Services resulted in EHR outages at all 400 sites for about three weeks, cost $67M in lost revenue & recovery.

SEPTEMBER 2020

Ransomware attack on Dusseldorf University Hospital causes relocation of patients and one death.

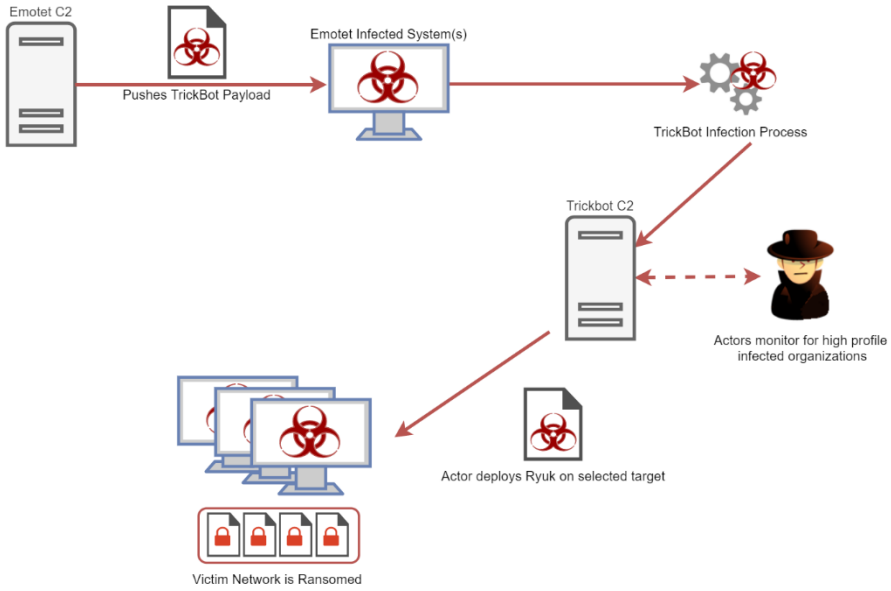
SEPTEMBER 2020

Maze ransomware ceases operations.

OCTOBER 2020

October 2020 – Disruption of Trickbot

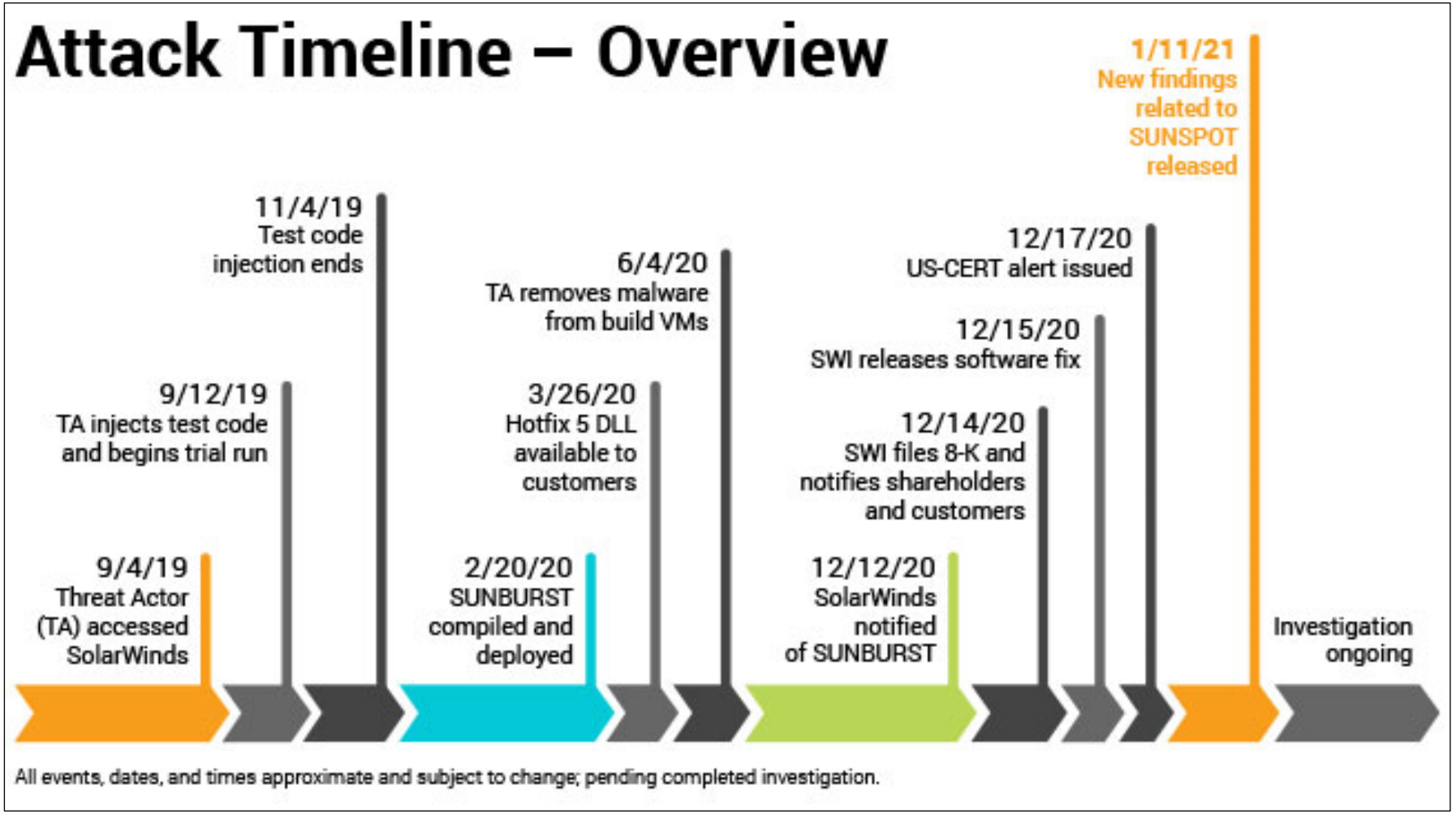
- Cyber Command conducted disruptive cyber operations against the TrickBot – specifically the command-and-control servers, starting on September 22.
    - It was speculated that this was to head off any potential cyberattacks during the 2020 Presidential election in November.
- Microsoft formed a coalition including ESET, Lumen's Black Lotus Labs, NTT, Symantec, and the Financial Services Information Sharing and Analysis Center (FS-ISAC).
    - Each of the organizations sent technical data to law enforcement to turn off parts of the TrickBot infrastructure, the idea being that if the C&C capability is shut down, TrickBot would be rendered useless.
- Microsoft launched another wave of disruptive attacks and is now claiming that they took down 94% of TrickBot's C2 infrastructure.
- They initially identified 128 command and control servers and eventually took down 120 of them.



December 2020 – SolarWinds

- Backdoor was included in malicious dynamic link library
  - Filename: SolarWinds.Orion.Core.BusinessLayer.dll (SUNBURST)
- SolarWinds download site password: SolarWinds123
- Malicious update dll is distributed to customers (manually or automatically)
- Compromised update signed with legitimate digital signature
- C2 Beaconing waits for several weeks after initial installation to begin
- SUNBURST backdoor is distributed to all customers via the standard software update distribution channels:

December 2020 – SolarWinds attack timeline



Emsisoft's 2020 numbers

- Emsisoft would later release data on the cost of ransomware in 2020:
  - Their data showed that the average ransom demand grew by more than 80%.
  - They tracked a minimum of $18.6 billion in ransom payments based on the data that they have access to – but they estimate the real total is around $75B globally.
  - They reported that the U.S. paid a minimum of about $1B but possibly as much as $3.7B.
  - They noted that these numbers go up significantly once you factor in downtime costs, and this may provide a little more insight as to why organizations pay ransom.
  - Including downtime costs, according to Emsisoft, U.S. victims paid a minimum of about $5B and are estimated to have paid as much as $20B.

Total cost: ransom demand costs + downtime costs

Country	Total Submissions	Minimum Cost (USD)	Estimated Costs (USD)
United States	15,672	$4,893,699,209	$19,574,796,838
France	4,476	$1,387,058,087	$5,548,232,346
Spain	4,088	$1,272,238,829	$5,088,955,314
Italy	3,835	$1,198,933,932	$4,795,735,727
Germany	3,747	$1,159,985,450	$4,639,941,801
Canada	3,236	$1,011,008,551	$4,044,034,203
U.K.	2,718	$838,750,742	$3,355,002,968
Australia	2,072	$648,093,574	$2,592,374,295
Austria	819	$256,822,720	$1,027,290,881
New Zealand	265	$82,569,552	$330,278,209

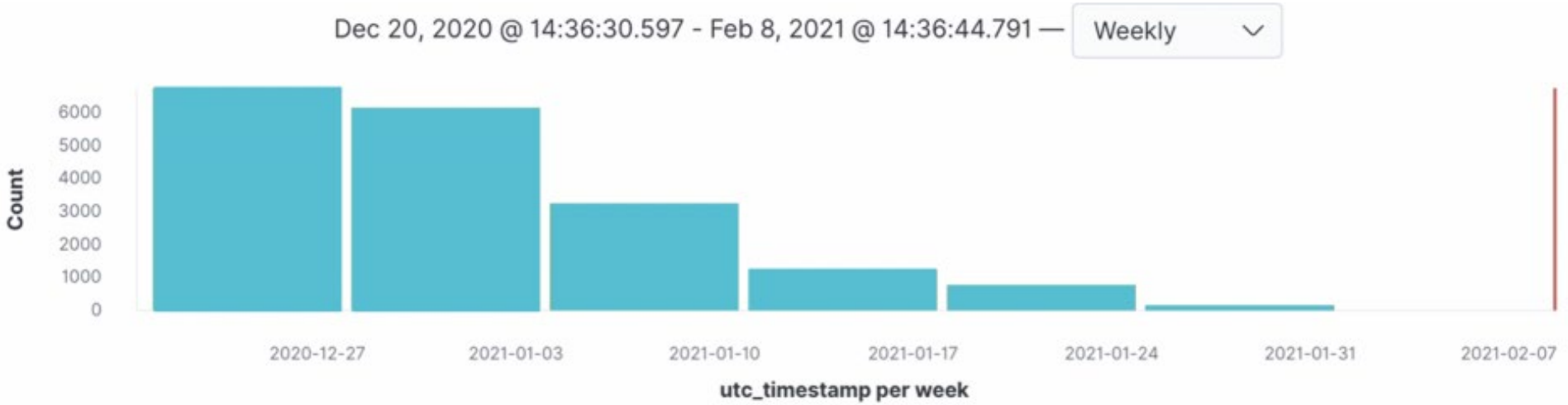
Other items of note for 2020:

- Per IBM research, the Sodinokibi (also known as Revil) operators:
  - Were the most active ransomware operators in 2020
  - Had revenues of $123M, their biggest single demand being $42M
  - Two-thirds of Sodinokibi's victims paid the ransom; 40% still had their data leaked anyway
  - 58% of Sodinokibi victims were based in the United States, the UK was second with 8%
- Per Palo Alto Unit 42, research on Covid-themed phishing:
  - Just under 70,000 coronavirus-themed phishing URLs were used in 2020
    - Most of them intended to steal business credentials
- Per Emsisoft research:
  - "In 2019, the U.S. was hit by an unprecedented and unrelenting barrage of ransomware attacks."
  - 2020 was the year of double extortion:
    - At the beginning of 2020, Maze was the only ransomware operators using double extortion
    - By the end of 2020, a total of 18 ransomware operators now engaged in double extortion
  - At least 560 healthcare facilities impacted in 80 separate ransomware incidents
  - PHI and other sensitive data was stolen and published online in at least 12 incidents

"2021 need not be a repeat of 2020. Proper levels of investment in people, processes and IT would result in significantly fewer ransomware incidents and those incidents which did occur would be less severe, less disruptive and less costly." — Fabian Wosar, CTO of Emsisoft.

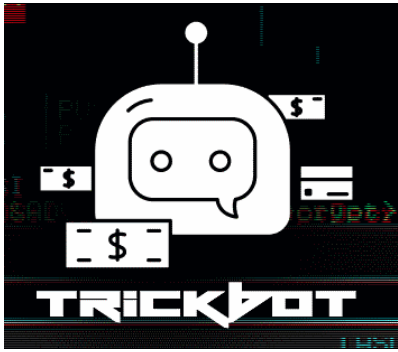
Emotet disruption

- International effort to takes down Emotet's global botnet infrastructure in late January
  - Included the U.S., Canada and several European countries
  - Video released by Ukrainian law enforcement shows raid with arrests and asset seizure
  - Authorities have pushed timed wiper for April 25th



FURTHER INFORMATION:
https://blogs.vmware.com/networkvirtualization/2021/02/death-of-emotet.html/
https://www.wired.com/story/emotet-botnet-takedown/
https://www.zdnet.com/google-amp/article/authorities-plan-to-mass-uninstall-emotet-from-infected-hosts-on-march-25-2021/

Healthcare Cybersecurity Events of Interest: January 2021, Part 2



- TrickBot is back!
  - Per a Menlo Security report, Trickbot launched a new attack campaign
  - Phishing campaign, targeting legal and insurance industry
- Adobe Flash reaches end-of-life
  - Final release: December 8, 2020
  - Flash content blocked by Flash Player on Jan 12, 2021
  - Adobe advises complete uninstallation of all instances
- Disruption of Netwalker by the Department of Justice
  - Department of Justice coordinated an international law enforcement effort to disrupt Netwalker
  - Canadian national alleged to be a member of Netwalker arrested in Florida
    - Accused of having been a part of stealing over $27M via ransomware
  - Seizure of ~$500K worth of cryptocurrency
  - Coordinated with the Bulgarian government to have the Netwalker leak website shut down
- Checkpoint research: Targeting of healthcare organizations globally increases over previous two months
  - 22% increase in targeting non-healthcare organizations; 45% increase in targeting healthcare organizations
  - Attacks against the health sector increased from 430 per week in October to 626 per week in November
  - Ryuk was the most frequently used ransomware variant to target healthcare and REvil was second
- FBI releases a Private Industry Notification on the aggressiveness of the Egregor ransomware operators

Accellion compromised by Clop Ransomware

- It was discovered in February that Accellion was breached by a Clop ransomware attack in December
  - Managed service provider focused on collaboration and secure file sharing
  - It's believed over 100 clients were impacted and at least 25 had data stolen
  - Targeted Accellion's legacy File Transfer Appliance (FTA)
  - Accellion agreed to $8.1 million settlement in January 2022
  - HC3 released an Analyst Note on the Accellion breach
  - At least Eleven healthcare organizations were impacted by the breach, some of which are:
    - Kroger Pharmacy: 1,474,284
    - Health Net: 1,236,902
    - Trillium Health Plan: 50,000
    - Arizona Complete Health: 27,390
    - Trinity Health (MI): Unknown
    - Stanford Medicine (CA): Unknown
    - The University of Miami Health (FL): Unknown
    - Centene Corp. (multiple companies): Unknown

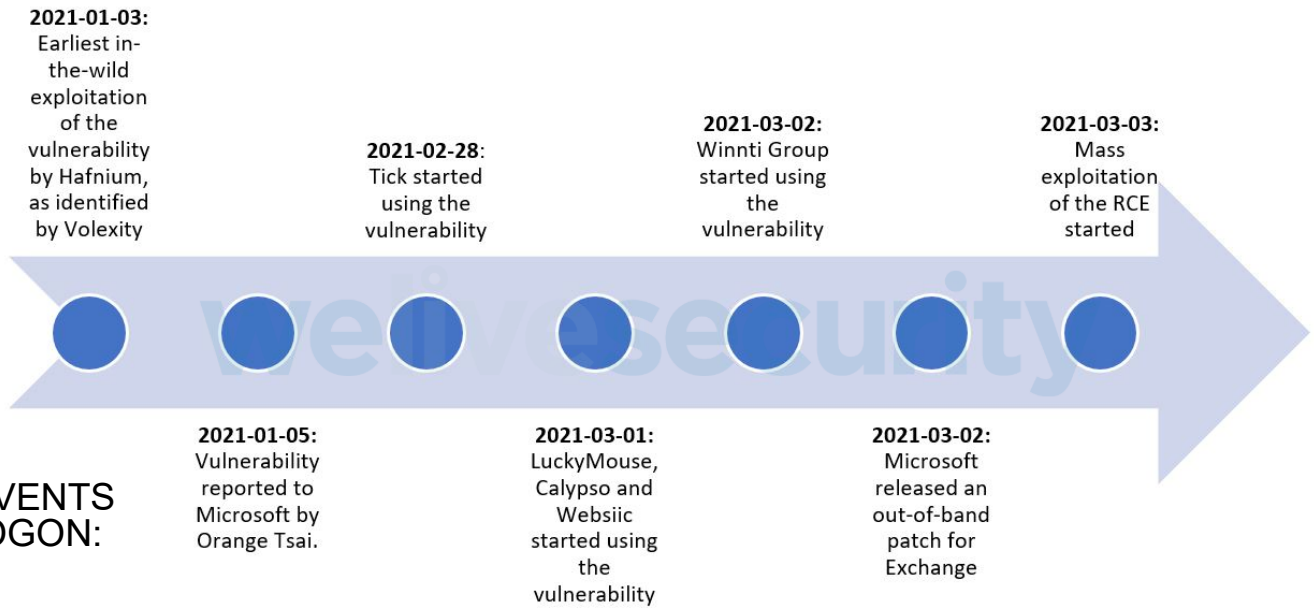
ProxyLogon vulnerabilities announced by Microsoft

- Microsoft released out-of-cycle, emergency patches for four high-priority, zero-day Exchange (versions 2013, 2016, and 2019) vulnerabilities that were being actively exploited at the time of release:
  - CVE-2021-26855 is a server-side request forgery vulnerability which allows an attacker to send arbitrary HTTP requests and authenticate to the exchange server
  - CVE-2021-26857 is a remote code execution vulnerability via insecure deserialization.
  - CVE-2021-26858 is a remote code execution vulnerability, more specifically a post authentication arbitrary file-write vulnerability. This requires either the exploitation of the first vulnerability (26855) or compromising legitimate administrative credentials first.
  - CVE-2021-27065 is a remote code execution vulnerability, in the form of a post authentication arbitrary file-write vulnerability.
- Microsoft attributed "with high confidence" the Chinese state-sponsored group, HAFNIUM, as attempting to exploit these vulnerabilities on US systems. HAFNIUM has been known to attack infectious disease researchers, among other targets. Also reported to be exploited by Tick, LuckyMouse, Winnti Group, Calypso and Websiic before Microsoft released patches
- HC3 Analyst note on ProxyLogon vulnerabilities can be found here.
- HC3 Analyst note on ProxyLogon detection tools can be found here.

FURTHER INFORMATION:
https://www.infosecurity-magazine.com/news/microsoft-patch-four-zeroday/
https://proxylogon.com/

ProxyLogon vulnerabilities were heavily exploited

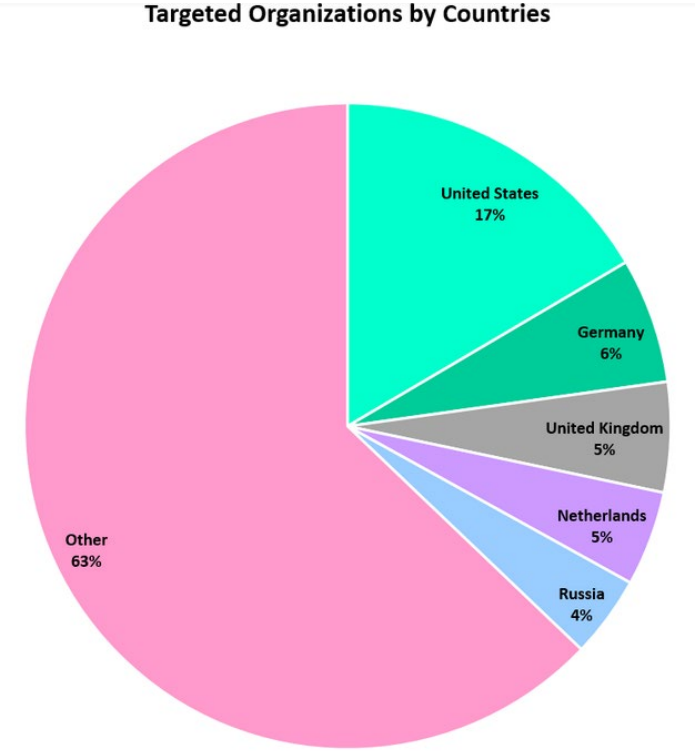
- The Lockfile ransomware gang were observed exploiting Proxylogon
- Two researchers noted that they have observed 34,000 vulnerable, Internet-facing exchange servers
  - 1900 were compromised over a 48-hour period
- Tech journalist Brian Krebs reported that at least 30,000 US organizations were attacked by China exploiting ProxyLogon vulnerabilities in the 72 hours following the patch release.
  - According to Krebs, the attackers deployed web shells on each system they compromised

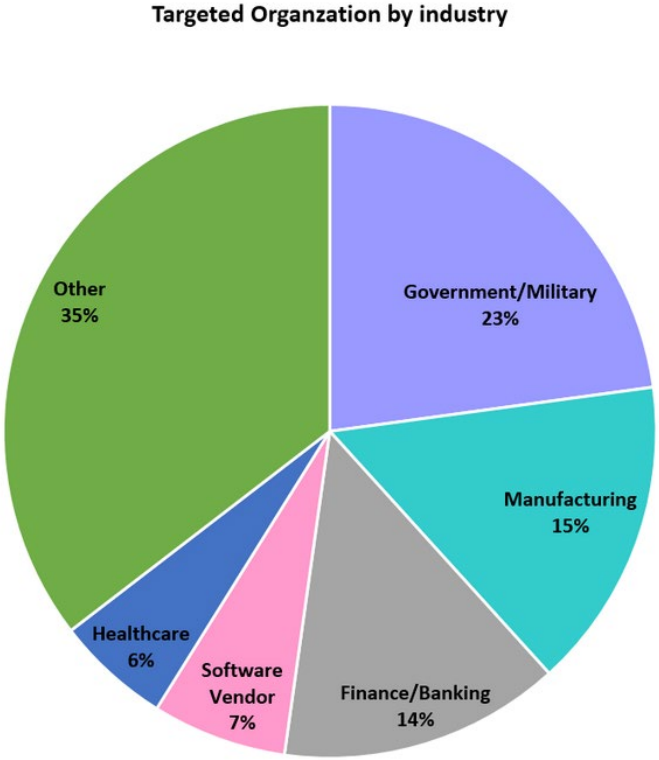


TIMELINE OF INITIAL EVENTS RELATED TO PROXYLOGON: (SOURCE: ESET)

CheckPoint research on ProxyLogon exploitation:

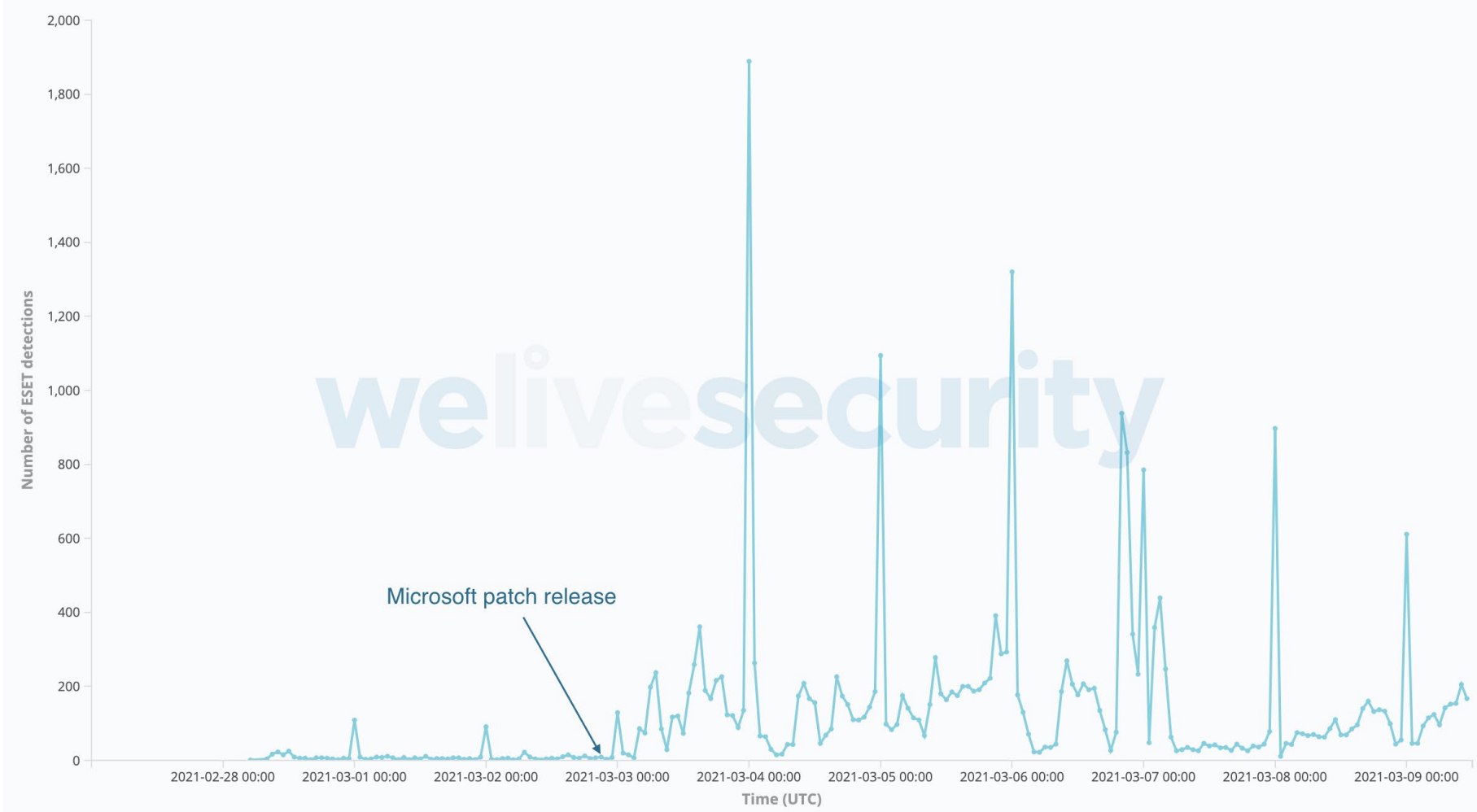
- CheckPoint posted a blog noting that attacks on vulnerable organizations double every two or three hours.
  - U.S. organizations have by far been the most targeted country with 17% of all attempted compromises.
  - Healthcare was one of the most targeted industries, accounting for 6% of all attacks.



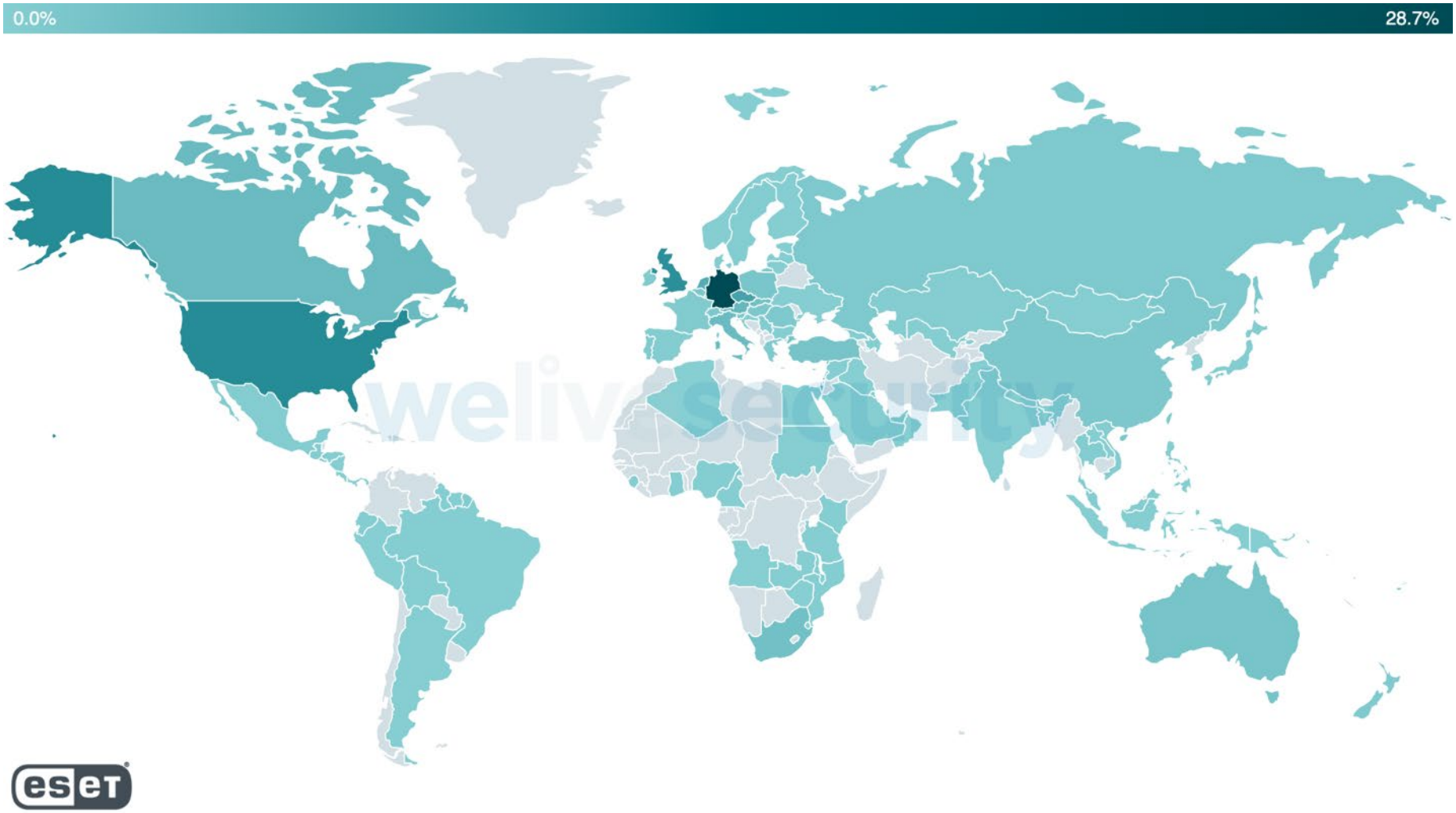


ProxyLogon exploitation followed by webshell drops:

Source: ESET

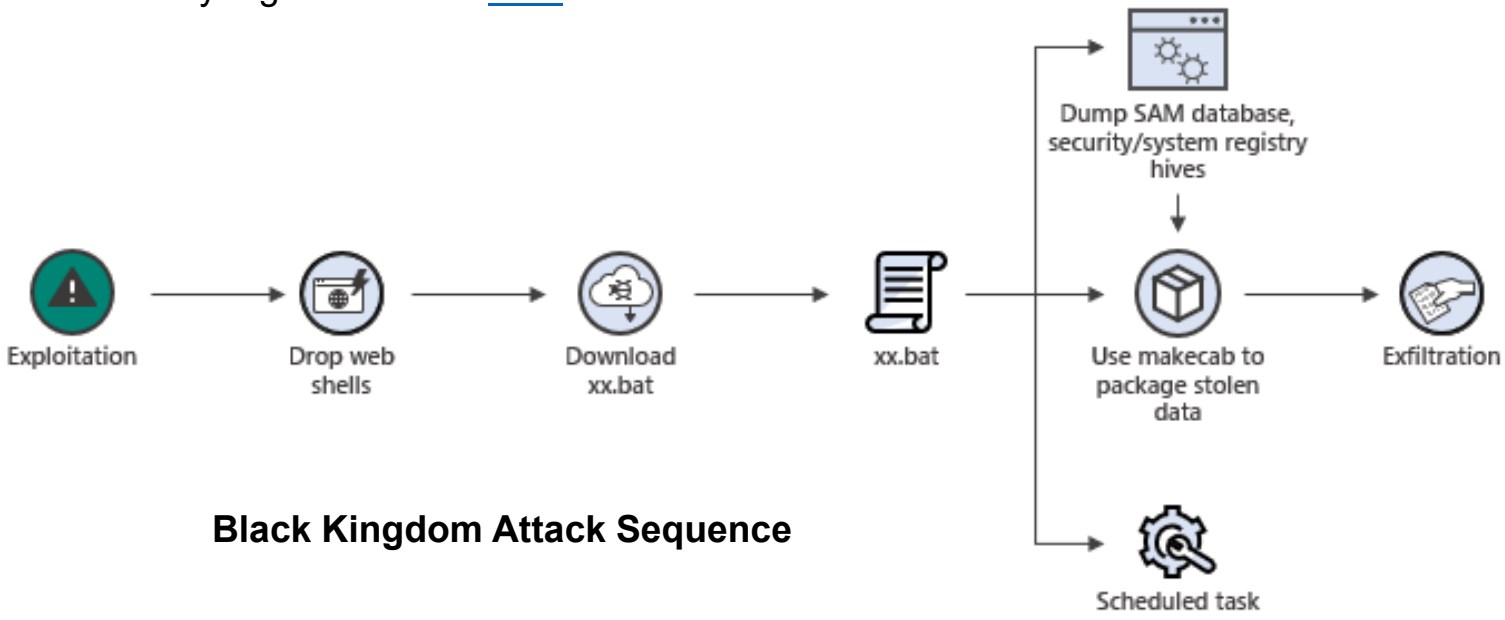


Geographic distribution of ProxyLogon webshell drops: Source: ESET



ProxyLogon vulnerabilities exploited by BlackKingdom/Pydomer:

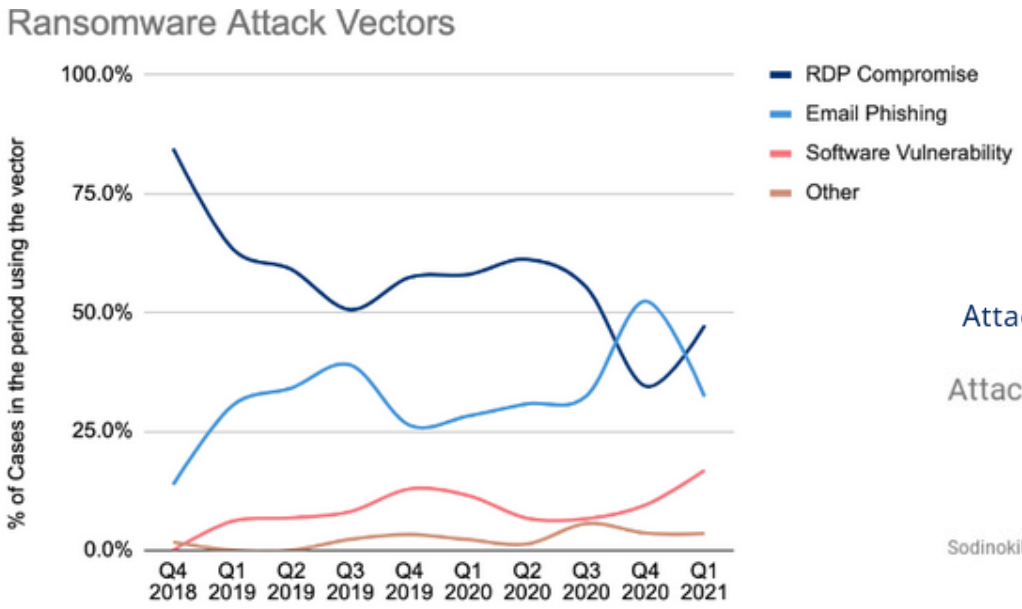
- A ransomware variant known as BlackKingdom was used in attacks leveraging the ProxyLogon vulnerability.
- According to Sophos, BlackKingdom is written in Python, and they traced it back to an IP address (TOR exit node) in Germany.
- According to Microsoft, the web shells dropped by the BlackKingdom operators were detected on at least 1,500 systems worldwide, and at least one of the ransom notes demands $10K in bitcoin.
- A timeline of ProxyLogon events is here.



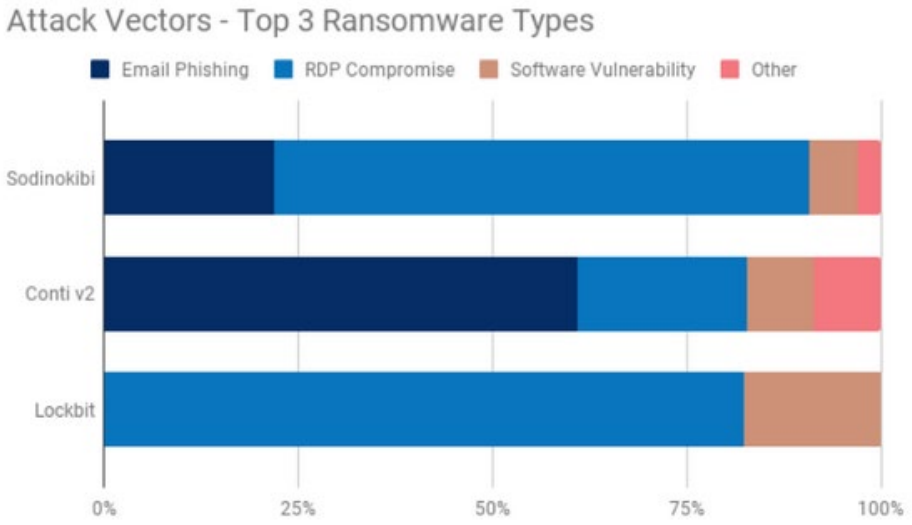
Black Kingdom Attack Sequence

Coveware Q1 data:

Most Common Ransomware Attack Vectors in Q1 2021



Attack Vectors used by the Top Three Ransomware Variants



Coveware Quarterly Ransomware Report: 2021 Q1

Average and Median Ransom Payments in Q1 2021

Average Ransom Payment

$220,298

+43% from Q4 2020

Median Ransom Payment

$78,398

+59% from Q4 2020

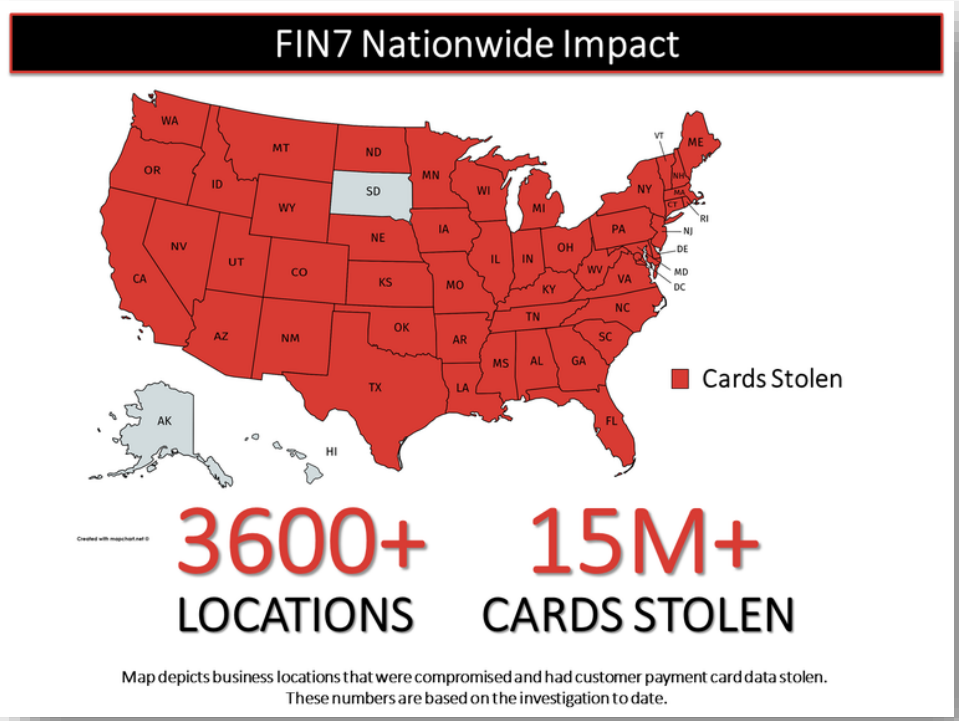
Most Common Ransomware Variants in Q1 2021

Rank	Ransomware Type	Market Share %	Change in Ranking from Q4 2020
1	Sodinokibi	14.2%	-
2	Conti V2	10.2%	+4
3	Lockbit	7.5%	+6
4	Clop	7.1%	New in Top Variants
5	Egregor	5.3%	-3
6	Avaddon	4.4%	+3
7	Ryuk	4.0%	-4
8	Darkside	3.5%	New in Top Variants
9	Suncrypt	3.1%	-1
9	Netwalker	3.1%	-5
10	Phobos	2.7%	-1

Top 10: Market Share of the Ransomware attacks

Sentencing of FIN7 System Administrator

- In January 2018, Fedir Hladyr, an alleged member of FIN7/Carbanak and a Ukrainian national, was arrested
  - He was extradited to the U.S. on charges related to alleged membership in cybercriminal group Carbanak/FIN7
  - He pleaded guilty to one count of conspiracy to commit wire fraud and one count of conspiracy to commit computer hacking; he was sentenced to 10 years in prison.
- Operating since at least 2015; believed to have ~70 members; alleged activities include both hacking and credit card fraud; estimates put Carbanak's theft between $1 billion and $5.7 billion.
- According to court documents, the gang stole 20 million credit card records from over 6,500 individual point-of-sale (PoS) terminals at more than 3,600 separate locations.
- https://therecord.media/fin7-hacker-sentenced-to-10-years-in-prison/



Emotet Takedown Complete

- Arrests were made and law enforcement took control of the Emotet infrastructure, authorities pushed an update which was scheduled to uninstall Emotet across its infrastructure at midnight on April 25th. Law enforcement distributed a new Emotet module in the form of a 32-bit EmotetLoader.dll. This was deployed via the standard Emotet deployment channels. When law enforcement took control of Emotet, they took control of their normal update channel.

Microsoft researchers identify BlocAlloc vulnerabilities:

- Microsoft's published research on a series of critical memory allocation vulnerabilities in IoT and OT devices that can be exploited to bypass security controls, leading to remotely execute arbitrary code or a system crash.
  - These are vulnerabilities in real-time operating systems (RTOS), embedded software development kits (SDKs), and C standard library (libc).
  - These vulnerabilities are associated with over 25 CVEs, have a CVSS score of 9.8 and apply to a number of domains including IoT, Industrial IoT, Operational Technology and IoMT.
  - CISA released an advisory (ICSA-21-119-04) listing the affected devices.
  - These vulnerabilities affected infusion pumps and wearable devices at a minimum.

Darkside Ransomware operators targeting stock prices:

- The Darkside operators began advertising on their dark web site for corrupt stock traders to work with.
  - Their plan is to partner up with stock traders who are willing to work with them, notify these partners after they have compromised a publicly traded company (but before a ransomware attack) so the trader can short the company, launch the ransomware attack, have the broker buy the shares back at the cheaper price and then split the profit.

CaptureRX Cyberattack

- CaptureRX is a pharmacy benefits management company that provides services such as prescription claims processing, patient assistance program administration, and public health service drug program administration.
  - Compromised by what was likely a combination of ransomware and data breach
  - At least 22 hospitals and healthcare providers have been affected by the breach and almost 2.5M victims have had their information leaked.

Scripps Cyberattack

- Scripps health network is San Diego's primary health system, a nonprofit that runs five hospitals and 19 outpatient facilities.
  - Attacked with ransomware; CEO confirmed that their systems were "damaged by malware"
  - Website disabled; Electronic health record access and online patient portal disrupted
  - Total cost of attack: $106.8M
    - ~$21 million in incident response and recovery costs
    - ~$91 million in lost revenues - they managed to recover about $6 million from their insurance.

Colonial Pipeline Ransomware Attack

- Colonial Pipeline: One of the nation's biggest pipeline operators
  - 2.5 million barrels/day (gasoline, diesel, home heating oil and jet fuel)
  - East coast (Linden, NJ to Houston, TX) – 5,500 miles; 45% of all fuel on east coast
- Department of Transportation' issued a regional emergency declaration for 17 states and Washington, D.C., to keep fuel supply lines open (relaxed fuel regulations regarding road transportation)
- Pipeline operations stopped immediately; ransom payment: $4.4 million; restored operations 6 days later
- Darkside RaaS (Ransomware-as-a-Service); attack began with a single compromised VPN password
- Brief fuel shortage, price spike; first time in 57-year history of pipeline that it was completely shut down
- The breached data contained names, contact information, date of birth, government-issued ID numbers and health-related information (including health insurance information)
- The Darkside operators shut down operations shortly after the attack, ostensibly due to the public scrutiny and political pressure on them; technical indicators point to a rebranding to the BlackMatter group

Executive Order on Cybersecurity

- The White House released an Executive Order on cybersecurity, outlining requirements for federal government and contractors.
  - Contractors will have new requirements to collect, preserve and report data related to compromises. Federal agencies required to implement modernization efforts and best practices such as:
    - Deployment of multi-factor authentication
    - More comprehensive deployment of strong encryption technologies
    - Rearchitecting their infrastructure for zero trust
    - Adopt secure cloud services (as much as practical)
    - Centralize and streamline access to cybersecurity incident data to drive analytics for identifying and managing cybersecurity risks and accelerate reporting
    - Establish baseline security standards for the development of software sold to the government
    - Establish a cybersecurity review board, composed of both government and private-sector members to analyze major incidents and make concrete recommendations afterwards
    - Create a standardized playbook for federal departments and agency incident handling, improve incident detection by further deployment of endpoint security systems


Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

Ransomware Attack on Irish Health Service Executive

- The Health Service Executive, Ireland's nationally publicly funded healthcare system, was attacked by ransomware
- Conti ransomware group carried out the attack; all IT systems were shut down; reverted to pen and paper
- National ambulance system continued operations; no interruption to COVID-19 vaccine appointments
- Conti also attempted an attack against Ireland's Department of Health, which apparently was not successful
- Most significant cyberattack in Irish government history
- Four months for full recovery
- HC3 developed a brief on the incident

Feidhmeannacht na Seirbhíse Sláinte
Health Service Executive

FURTHER INFORMATION:
https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

Department of Homeland Security: New Cybersecurity Requirements for Critical Pipeline Owners/Operators

- The Department of Homeland Security released a directive requiring critical pipeline owners/operators to report cybersecurity incidents to them and require them to designate cybersecurity coordinators and to report risks, security gaps, and remediation measures to the federal government within 30 days.

Justice Department elevates ransomware cases to the same priority given to terrorism

- A memo was circulated throughout U.S. attorney's offices across the country which required that information about ransomware investigations in the field to be centrally coordinated with a Washington DC-based task force.
- Investigators in U.S. attorney's offices around the country handling ransomware attacks will be expected to share both updated case details and active technical information with leaders in Washington.

Department of Justice charges Latvian national with being part of Trickbot

- The Department of Justice announced that a Latvian-national was charged with 19 counts in an indictment for her role with Trickbot including conspiracy to commit computer fraud and aggravated identify theft
- She was previously arrested in Miami, charged with being a developer, and specifically having written code to control, deploy and manage payments. She was also accused of having provided the Trickbot Group with the code needed to monitor and track authorized users and she also stands accused of having developed the tools and protocols required to store login credentials stolen from victims' networks.

Avaddon ransomware shuts down and releases decryption keys

- The Avaddon ransomware operators released just under 3,000 decryption keys – one for each of their victims – which were confirmed to be valid. Also, all their TOR sites became inaccessible.
- Avaddon was in operation for 12 months, and were the subject of alerts by both the FBI and Australian law enforcement.

Putin Says Russia Might Accept Conditional Handover of Cyber Criminals

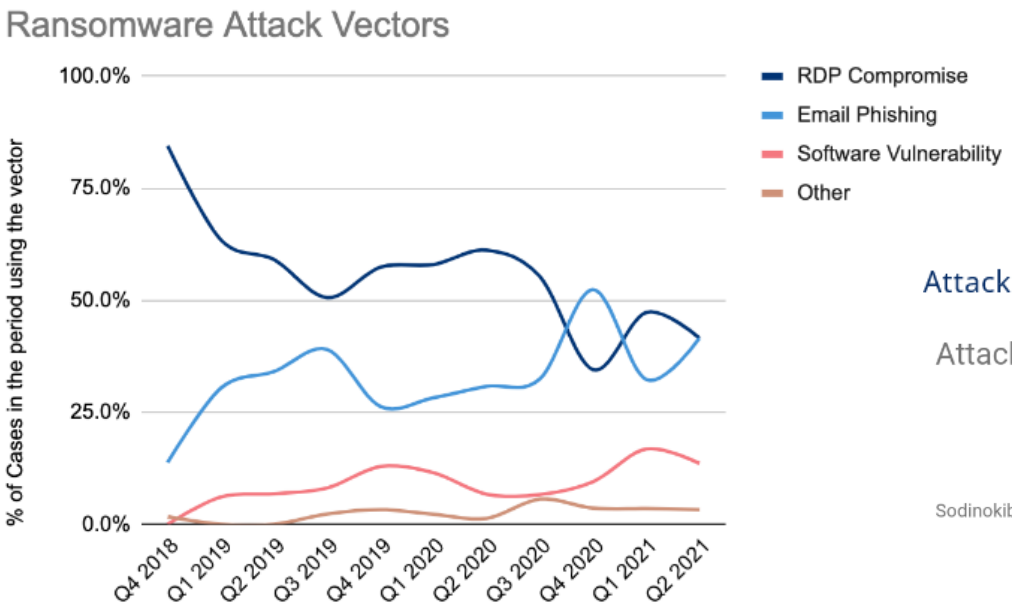
- Russian President Putin made comments that aired on Russian state television, which indicated that he would be ready to hand over cyber criminals to the U.S. if the U.S. did the same for Russia and the two powers reached an agreement to that effect.
- Presidents Biden and Putin held a summit in Geneva, Switzerland and discussed ransomware.

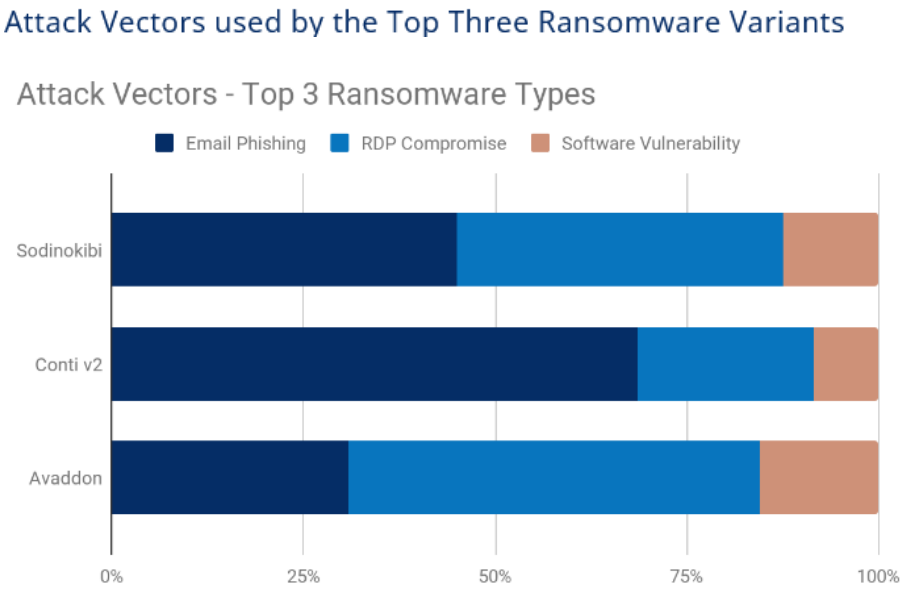
PrintNightmare

- Techical details of a Windows remote code execution print vulnerability as well as a proof-of-concept (PoC) exploit were accidentally leaked by researchers:
  - CVE-2021-34527
- This exploit requires authentication, but it's still a severe issue because it allows attackers to use it to take over a Windows domain controller and then potentially deploy malware across a company's network

Coveware Q2 Data:

Most Common Ransomware Attack Vectors in Q2 2021





Coveware Quarterly Ransomware Report: 2021 Q2

Average and Median Ransom Payment Amounts Declined in Q2 2021

Average Ransom Payment

$136,576

-38% from Q1 2021

Median Ransom Payment

$47,008

-40% from Q1 2021

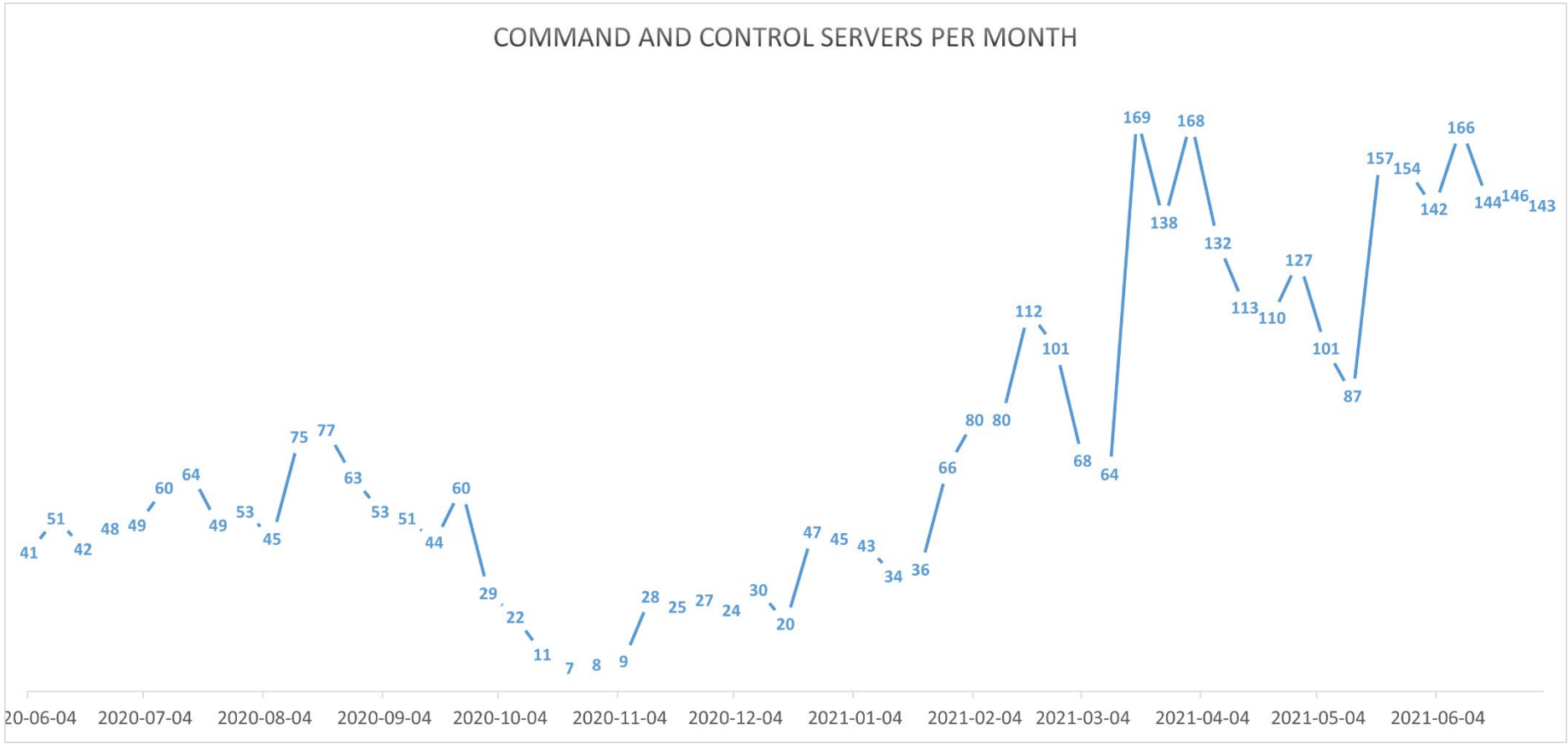
Most Common Ransomware Variants in Q2 2021

Rank	Ransomware Type	Market Share %	Change in Ranking from Q1 2021
1	Sodinokibi	16.5%	-
2	Conti V2	14.4%	-
3	Avaddon	5.4%	+3
4	Mespinoza	4.9%	New in Top Variants
5	Hello Kitty	4.5%	New in Top Variants
6	Ryuk	3.7%	+1
7	Clop	3.3%	-3
8	THT v2	2.9%	New in Top Variants
9	LV	2.5%	New in Top Variants
9	Zeppelin	2.5%	New in Top Variants

Top 10: Market Share of the Ransomware attacks

BitDefender: TrickBot is back

- The company BitDefender published research on Trickbot
- This research implies that the TrickBot operators are trending towards full operations once again

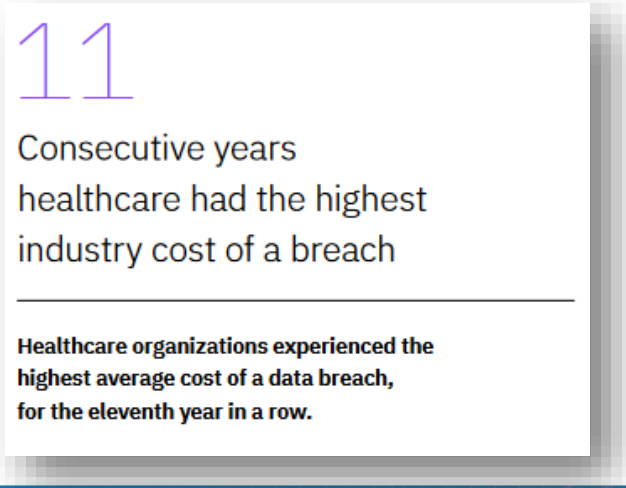


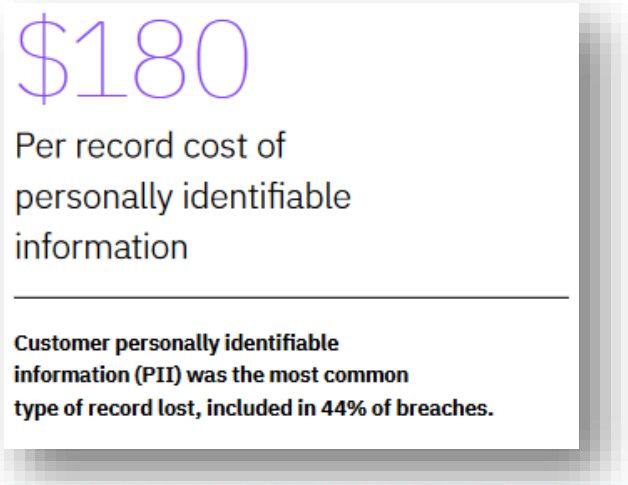
Kaseya VSA Ransomware Attack

- Kaseya is an IT managed service provider that was attacked by the REvil/Sodinokibi operators.
- Specifically, the virtual systems administrator (VSA) platform was compromised.
  - Kaseya sells the VSA to managed service providers, who then use it to support their customer base.
- It is believed that between 50 and 60 of their customers were impacted, and those 50 or 60 customers manage IT services for about 1,500 companies worldwide.
- The company announced that they had obtained a decryption key for its own systems and those of its customers.
  - They did not name the source of the key, they just called them a “trusted third party”.
- Initially, the attackers demanded $70 million for the key but quickly dropped their demands to $50 million, and it is not known if any amount was ever paid.

IBM Annual Data Breach Cost Report

- IBM released their 2021 Cost of a Data Breach report
- They assessed that the data breaches in 2021 cost a company $4.24 million per incident on average, which is the highest figure in the 17-year history of this report.
  - In the United States, data breach costs averaged about $9 million per incident.
  - The cost of breaches increased about 10% in a year, and IBM largely attributes that to the remote workforce which has increasingly been in place since the beginning of the pandemic.
  - On that note, IBM also found that the average cost of a breach increased about $1 million when remote work was a factor in the breach.
- The average healthcare breach was $9.23 million, which was a dramatic increase, about 30%, from $7.13 million in 2019.





Biden Administration Anti-ransomware Actions:

- Stopransomware.gov launched – intended to be a hub of resources for the public to defend against ransomware.
- The Department of State announced a $10 million reward for information related to the identification of state-sponsored cyber attackers as part of their Rewards for Justice Program. Specifically, these actions include:
  - Transmitting extortion threats as part of a ransomware attack
  - Intentional unauthorized access to a system to obtain information from it
  - Knowingly transmitting code or commands which cause damage to a system
- The White House announced a cross-government task force to coordinate both offensive and defensive measures against ransomware attacks
  - Some of the responsibilities of the task force include:
    - Promoting digital resilience among critical infrastructure companies
    - Working to halt ransom payments made through cryptocurrency platforms
    - And coordinating various actions with U.S. allies
- The U.S. and allies attributed the Microsoft Exchange (ProxyLogon) hacking campaign to China
  - The attacks targeted over a quarter of a million Exchange servers worldwide
- The Justice Department released an indictment for four members of the Chinese cyber threat group APT40 for cyberattacks related to theft of trade secrets and intellectual property

BlackMatter

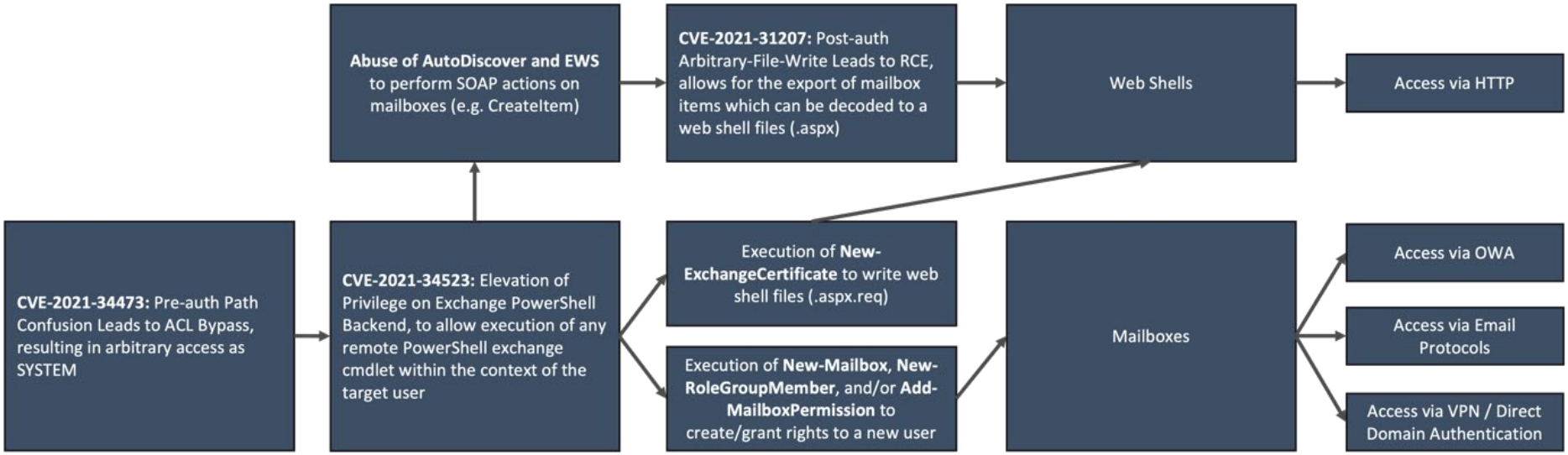
- The Backmatter ransomware gang begins operations
  - Speculation is that they are either a rebranded version of a previous group, or they at least consist of members with significant operational experience.
    - REvil? Speculation they disbanded after the Kaseya attack
    - Darkside? Claimed to disband after the Colonial Pipeline attack
  - Initial analysis is they are organized and prepared for operations early with an operational leak site, and several darkweb advertisements looking to purchase corporate access with significant cryptocurrency deposits
  - They claim to have highly capable ransomware capable of compromising multiple platforms

PwnedPiper

- Armis identified nine vulnerabilities in pneumatic tubes produced by TransLogic which are collectively referred to as PwnedPiper. TransLogic PTS are believed to be present in more than 2,300 hospitals in North America.
- That research revealed that an unauthenticated attacker could gain full control over TransLogic pneumatic tube systems that are connected to the internet and then compromise the entire tube network of a hospital.
- The vulnerabilities cover a variety of potential impacts including password leakage, remote code execution, denial-of-service, and full device compromise. Firmware has been available to address them since August.

ProxyShell Vulnerabilities Impacting MS Exchange Servers

- Three chained Microsoft Exchange vulnerabilities were briefed at the Black Hat conference. They are collectively called ProxyShell and they allow for unauthenticated, remote code execution.
- CVE-2021-34473 - Pre-authentication Path Confusion leads to Access control list Bypass
- CVE-2021-34523 - Elevation of Privilege on Exchange PowerShell Backend
- CVE-2021-31207 - Post-authentication Arbitrary-File-Write leads to RCE
- The first two were patched in April and the third was patched in May, but apparently there are a lot of unpatched Exchange servers connected to the Internet



Trickbot Developer Arrested

- An alleged Trickbot developer was arrested in South Korea. He claimed that he did not know he worked for a cybercrime gang after getting hired from an employment site.
- 38-year old Vladimir Dunaev was alleged to be a malware developer that supervised the creation of TrickBot's browser injection module. He is facing charges that could get him 60 years in prison.

United Health Centers falls victim to ransomware attack by Vice Society

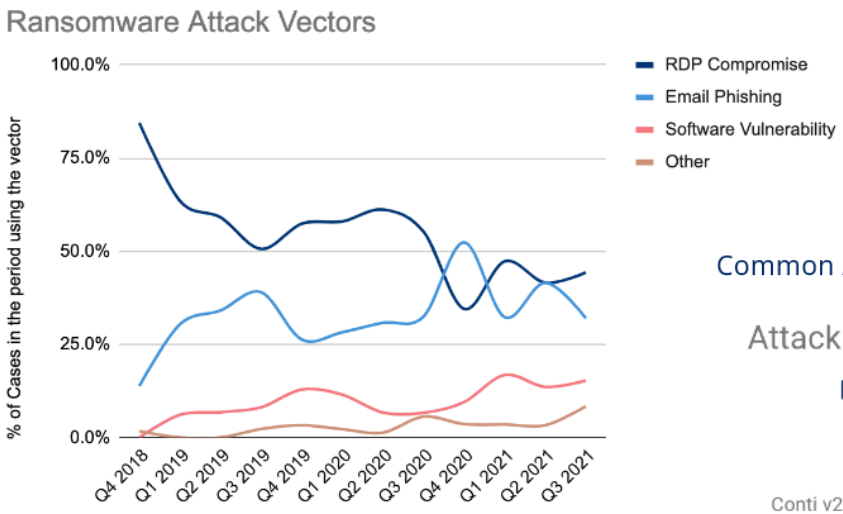
- The Vice Society Ransomware gang compromised United Health Centers
- The attack caused disruptions of IT systems across all their locations and they have been in the process of reimaging their systems and attempting to recover from offline backups
- They leaked UHC files from UHC including PHI

Cyberattack on Alabama hospital linked to 1st alleged ransomware death

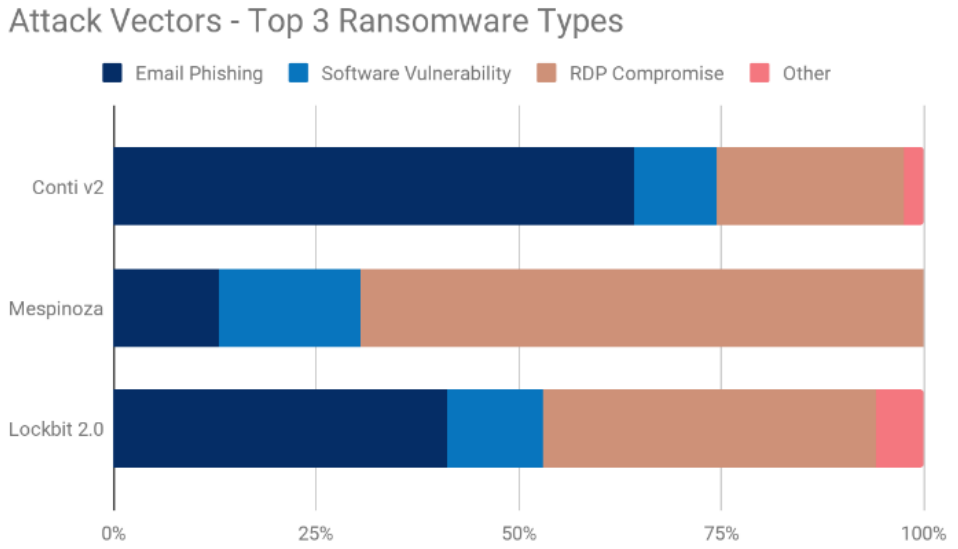
- According to a lawsuit filed against Springhill Medical Center of Alabama, a ransomware attack that caused the facility to facility shut down its network for almost eight days is alleged to have caused the death of a baby.
- A baby was born at the hospital with her umbilical cord wrapped around her neck. The baby suffered severe brain damage as a result, and she died nine months later due to related complications.
- The doctor who delivered the baby texted the nurse manager that she would have delivered the baby by cesarean section had she seen the monitor readout.

Coveware Q3 data:

The Most Common Ransomware Attack Vectors in Q3 2021



Common Attack Vectors used by the top 3 Ransomware Variants in Q3 2021



Coveware Quarterly Ransomware Report: 2021 Q1

Average Ransom Payment Amounts Flat in Q3 2021

Average Ransom Payment

$139,739

+2.3% from Q2 2021

Median Ransom Payment

$71,674

+52.5% from Q2 2021

The Most Common Ransomware Variants in Q3 2021

Rank	Ransomware Type	Market Share %	Change in Ranking from Q2 2021
1	Conti V2	19.2%	+1
2	Mespinoza	11.3%	+2
3	Sodinokibi	8.9%	-2
4	Lockbit 2.0	8.4%	New in Top Variants
5	Hello Kitty	5.4%	-
6	Zeppelin	4.4%	+3
7	Ranzy Locker	3.0%	New in Top Variants
8	Suncrypt	2.5%	New in Top Variants
8	Hive	2.5%	New in Top Variants
9	Ryuk	2.0%	-3
9	BlackMatter	2.0%	New in Top Variants

Top 10: Market Share of the Ransomware attacks

Biden Announces 30-Country Coalition Against Ransomware

- The Biden administration convened a meeting of 30 countries to collaborate against ransomware operators incuding improving law enforcement cooperation, reducing illicit use of cryptocurrency and diplomatic engagement.

FinCEN report: Top 10 ransomware groups responsible for 5.2 billion in transactions

- The Treasury Department's Financial Crimes Enforcement Network (FinCEN) released a report on ransomware trends. They examined 177 wallet addresses tied the top 10 ransomware gangs and noted that they have extorted $5.2 billion dollars total since they've been operating. In the first half of 2021 – they extorted a total of $1.56 billion.

Man sentenced to 7 years in prison for hacking healthcare provider

- Justin Sean Johnson, known online as TheDearthStar and Dearthy Star, was sentenced to seven years in prison for the 2014 hack of the University of Pittsburgh Medical Center. He was convicted of having breached UPMC's human resources databases, stealing PII and W-2 info associated with over 65,000 employees, which he subsequently sold on the dark web.

REvil ransomware operators claim to be shutting down operations

- A REvil operator claimed in a conversation with Recorded Future Analyst Dimitry Smilyanets that the group was shutting down. Their dark web/Tor sites were taken down by a coalition of law enforcement agencies.

BlackMatter

- Darkside ransomware operators have moved approximately 107 BTC ($6.8M) to other wallets about six hours after reports broke that a coalition of law enforcement agencies hijacked the servers of REvil. Members of the group later published a public notification that they were disbanding due to law enforcement pressure.

State Department – Rewards for Justice Program

- The Department of State announced a $10,000,000 reward for the identification or location of DarkSide ransomware members (or any rebrand group) operating in key leadership positions.
- A reward of $5,000,000 is also being offered for information leading to the arrest of any individual who attempts to participate in a Darkside attack.

Europol detains suspects behind LockerGoga, MegaCortex, and Dharma ransomware attacks

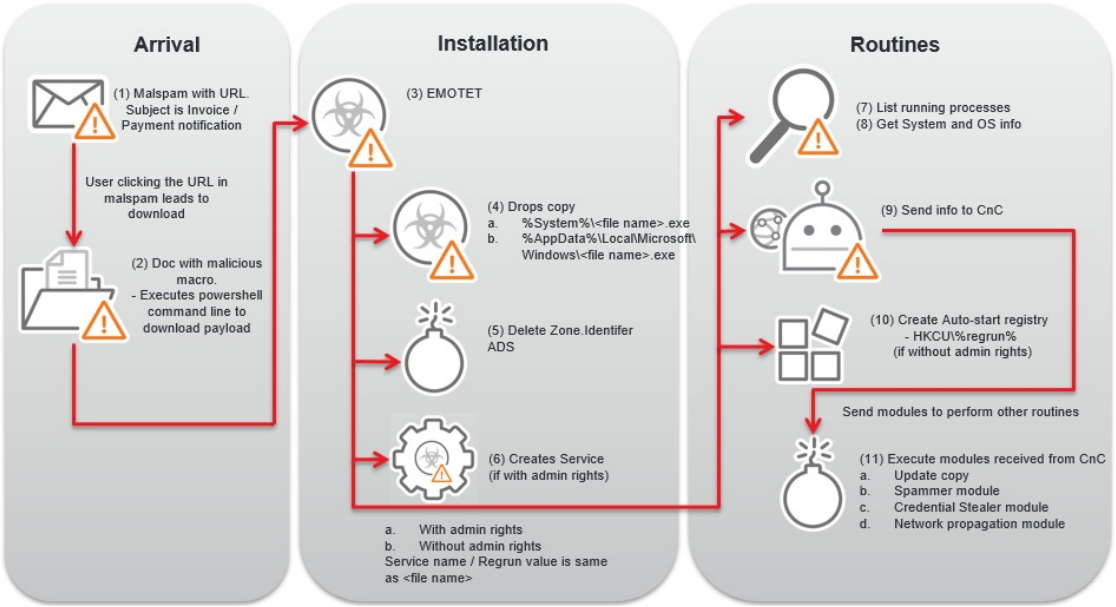
- Europol, the EU's top law enforcement agency arrested 12 people accused of engaging in ransomware operations. They were accused of deploying a number of ransomware strains including LockerGoga, MegaCortex and Dharma as well as using other malware variants including Trickbot and post-exploitation tools such as Cobalt Strike. Their accusations include launching attacks against 1800 victim organizations across 71 countries since 2019. The arrests involved efforts by eight countries, including the US.

The government pressure continued…

- Romanian law enforcement arrested two suspects believed to be REvil ransomware affiliates
- Kuwaiti authorities arrested a GandCrab ransomware affiliate (predecessor to REvil), the three of them combined are suspected of being behind roughly 7,000 attacks demanding over $200 million in ransoms.
- The Department of Justice (DoJ) unsealed two grand jury indictments for two individuals associated with the REvil ransomware group. One of those individuals was arrested in Poland, which maintains an extradition treaty with the United States. also announced they seized more than $6M in cryptocurrency from one of the indicted operators
- The Department of State announced a reward of up to $10 million for information leading to the identification or location of any individual holding a key leadership position in the REvil ransomware group.
    - 7 REvil operators or affiliates have been arrested since February
- The US Treasury Department announced sanctions yesterday on the cryptocurrency exchange Chatex for "facilitating financial transactions for ransomware actors". They asserted that over half of the transactions on the exchange are directly traced to illicit or high-risk activities such as darknet markets, high-risk exchanges, and ransomware"

Emotet is back

- Emotet is active again - its back and rebuilding its infrastructure. Security researchers and companies have been releasing small indications of its activity on social media
- It appears to have new and updated capabilities:
  - Changes to the loader – new commands are available for it.
  - Changes to the dropper capability.
  - New command and control infrastructure operational
    - 246 systems believed to be part of it



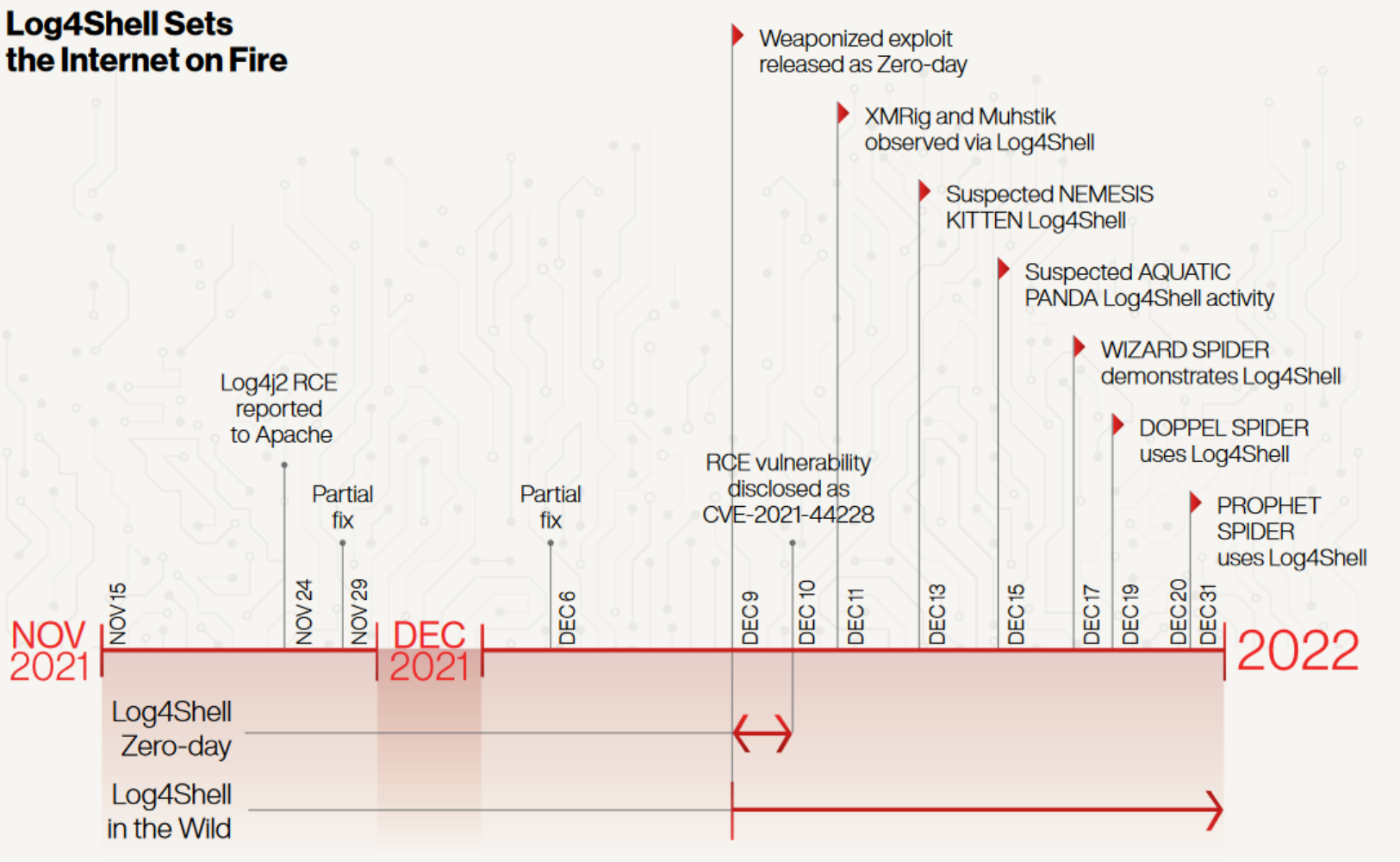
Log4J

- Log4J is a Java-based, ubiquitous logging tool now known to have multiple vulnerabilities, including multiple remote code execution flaws that can provide an attacker total control of a system.
- Initially discovered in November 2021, multiple Log4J updates have been released since then.
- No major compromises in the health sector to date; however, the health sector remains highly vulnerable, as do other industries.
- Health sector adversaries are actively leveraging these vulnerabilities.
- Updating can be a time-consuming and tedious process.
- Further vulnerabilities may continue to be identified soon.
- There are both short- and long-term steps to take in order to remain secure.
- Vulnerabilities in ubiquitous apps will present similar issues in the future.

Five vulnerabilities in Log4J (plus one in Logback framework)

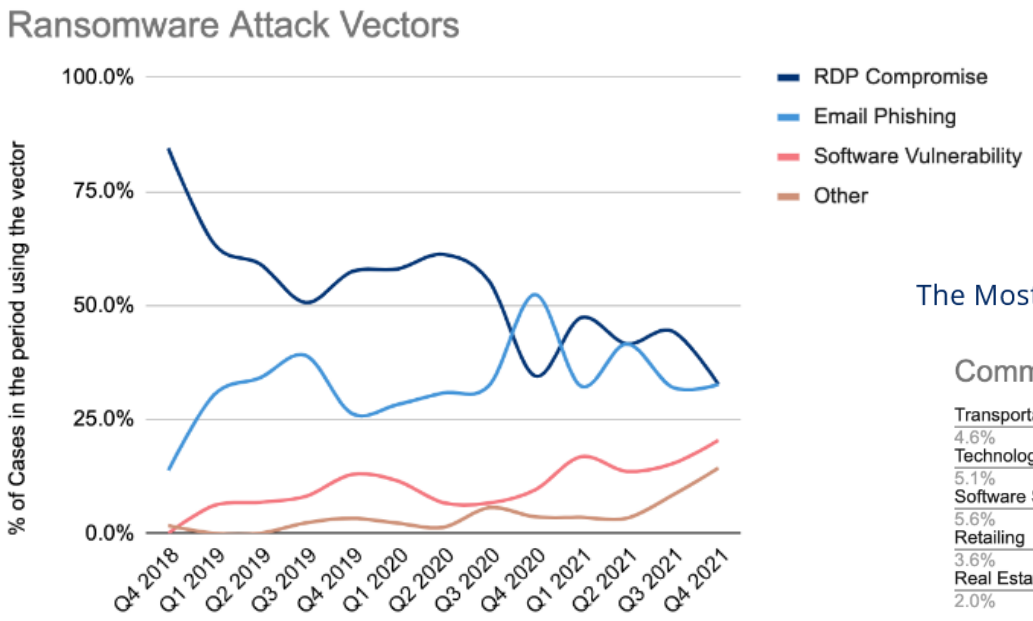
CVE	TYPE	Description/Notes
CVE-2021-44228	Remote Code Execution	Rated Critical; present in Log4j2 2.0-beta9 to 2.12.1 and 2.13.0 through 2.15.0; called Log4Shell; CVSS: 10 of 10; fixed in version 2.15.0
CVE 2021-45046	Denial of Service	Fix to address CVE-2021-44228 in 2.15.0 was incomplete in certain non-default configurations; fixed in version 2.16.0
CVE-2021-4104	Remote Code Execution	Rated High; present in versions 1.x; CVSS: 7.5; fixed in version 2.17.0 (no fix for Log4J version 1 - EoL)
CVE-2021-42550	Arbitrary Code Execution	Rated Moderate; present in Logback logging framework (successor to the Log4j 1.x); fixed with Logback versions, 1.3.0-alpha11 and 1.2.9
CVE-2021-45105	Denial of Service	Versions 2.0-alpha1 through 2.16.0 did not protect from uncontrolled recursion from self-referential lookups; CVSS: 7.5 of 10; fixed in version 2.17.0
CVE-2021-44832	Remote Code Execution	Present in version 2.17.0; CVSS score of 6.6; fixed in version 2.17.1

Log4Shell timeline

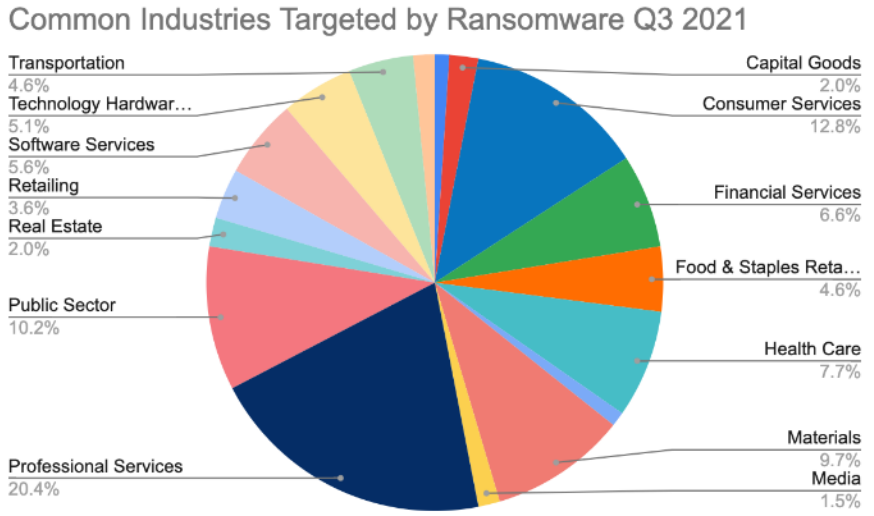


Coveware Q4 data:

The Most Common Ransomware Initial Ingress Vectors in Q4 2021



The Most Common Industries Impacted by Ransomware in Q4 2021



Coveware Quarterly Ransomware Report: 2021 Q4

Average Ransom Amount up Sharply in Q4 2021

Average Ransom Payment

$322,168

+130% from Q3 2021

Median Ransom Payment

$117,116

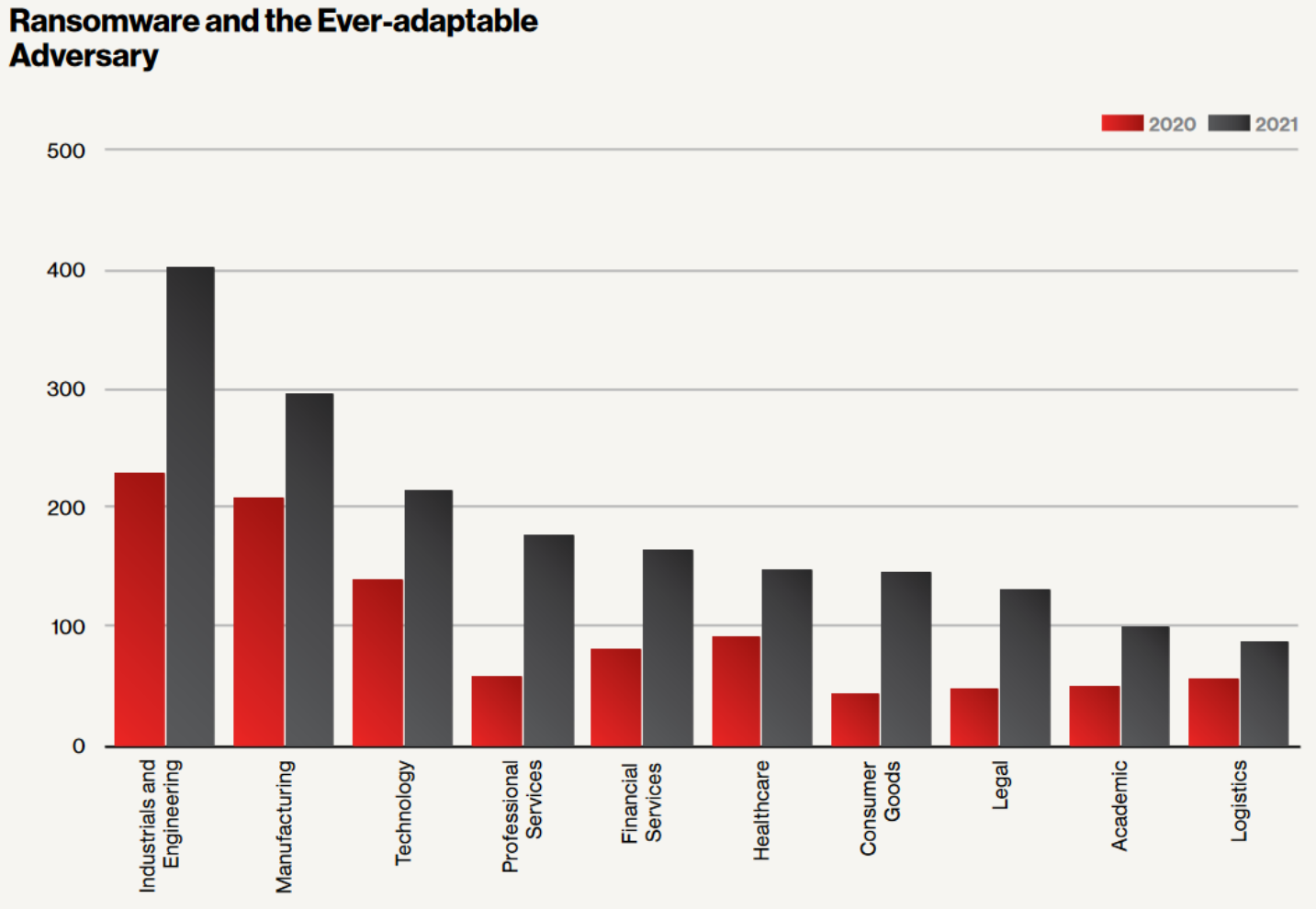
+63% from Q3 2021

The Most Common Ransomware Variants in Q4 2021

Rank	Ransomware Type	Market Share %	Change in Ranking from Q3 2021
1	Conti V2	19.4%	-
2	LockBit 2.0	16.3%	+2
3	Hive	9.2%	+5
4	Mespinoza	4.1%	-2
5	Zeppelin	3.6%	+1
5	BlackMatter	3.6%	+4
6	Karakurt	3.1%	New in Top Variants
6	Suncrypt	3.1%	+2
6	AvosLocker	3.1%	New in Top Variants

Top 10: Market Share of the Ransomware attacks

2021 Ransomware as compared to 2020:



What does all this mean for healthcare cybersecurity for 2022 and beyond?

- The continuation of conventional wisdom and existing trends applies in many cases
  - **Healthcare organizations should continue to defend against phishing**
    - Training and employee awareness
      - Current events can and do serve as themes for phishing campaigns
    - Phishing test programs
    - Gateway/mail server filtering
    - Blacklisting/whitelisting
    - Operationalization of indicators of compromise
  - **Remote access technologies should be locked down**
    - Virtual Private Networks and technologies leveraging the Remote Desktop Protocol should be operationally minimized
    - Turn off services where they are not needed
    - Limit services to only when they are needed
    - Log and periodically review activity
    - Update all tools as soon as updates are released
    - Always apply the principle of least privilege

What does all this mean for healthcare cybersecurity for 2022 and beyond?

- The continuation of conventional wisdom and existing trends applies in many cases (continued)
  - **Vulnerability Management**
    - Situational awareness begins with knowing your own infrastructure
      - Develop and aggressively maintain enterprise asset inventory
      - Must be systematic – comprehensive and repeatable
      - Must have mechanisms of enforcement
    - Maintain situational awareness of applicable vendor updates and alerts
    - Develop repeatable testing, patching and update deployment procedures
  - **Understand the value of what your organization has to offer to the adversary**
    - Patient records/PII/PHI can be sold for a high price
    - If you operate in such a way that you can be disrupted then you can also be extorted
    - Foreign countries may want/need your intellectual property
  - **Operate with resilience in mind**
    - High probability of compromise
    - What will you do if it happens?
    - Incident response
    - Continuity of Operations (COOP)

What does all this mean for healthcare cybersecurity for 2022 and beyond?

- Relatively new(ish) ways of thinking about defense
  - **Distributed attack vectors**
    - Adversaries are thinking in terms of maximizing their victims with a single attack
      - Managed service provider compromise
      - Supply chain compromise
      - Software components
    - Examples: Solar Winds, Kaseya, Log4J
    - How to prevent and mitigate?
      - Request MSPs to enumerate the their security capabilities
      - Request software bill of materials
      - Develop/implement/test contingency plans
      - Most important: Think in terms of how you can be compromised by your suppliers, vendors, business partners, customers and service providers
  - **The government can help you; You still have the most important role in defending yourself**
    - Diplomacy, law enforcement and other government actions have been impactful
      - Technical disruptions, arrests, bounties
    - The cybercriminal ecosystem is resilient
      - As long as there are victims to compromise there will be someone willing to try

- Moving through 2022 and beyond…
  - Situational awareness will continue to be more and more important…
    - New threats and their tactics, techniques, procedures and weapons
    - New vulnerabilities and the means to correct them or mitigate exploitation
  - Maintaining trusted defense measures
  - Defending against distributed attacks and other new avenues of compromise
- Government resources:
  - DHS/CISA Stop Ransomware: https://www.cisa.gov/stopransomware
  - FBI Cybercrime: https://www.fbi.gov/investigate/cyber
  - FBI Internet Crime Complaint Center (IC3): https://www.ic3.gov/Home/ComplaintChoice/default.aspx/
  - HC3 Products: https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html

Reference Materials

References

IBM X-Force Threat Intelligence Index 2021
https://ibm.ent.box.com/s/hs5pcayhbbhjvj8di5sqdpbbd88tsh89

Fake Websites Used in COVID-19 Themed Phishing Attacks, Impersonating Brands Like Pfizer and BioNTech
https://unit42.paloaltonetworks.com/covid-19-themed-phishing-attacks/

Another banner year for cybercriminals
https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/

Trickbot Malware: new year—old lure
https://www.menlosecurity.com/blog/trickbot-new-year-old-lure

Trickbot is back again - with fresh phishing and malware attacks
https://www.zdnet.com/article/trickbot-is-back-again-with-fresh-phishing-and-malware-attacks/

Adobe Flash Player EOL General Information Page
https://www.adobe.com/products/flashplayer/end-of-life.html

Adobe Flash reaches end-o-life
https://www.infoworld.com/article/3601062/adobe-flash-reaches-end-of-life.html

NetWalker ransomware investigation yields arrest, big cryptocurrency seizure
https://www.cyberscoop.com/netwalker-us-bulgaria-canada

Department of Justice Launches Global Action Against NetWalker Ransomware
https://www.justice.gov/opa/pr/department-justice-launches-global-action-against-netwalker-ransomware

Trickbot is back again - with fresh phishing and malware attacks
https://www.zdnet.com/article/trickbot-is-back-again-with-fresh-phishing-and-malware-attacks/

References

Chainalysis in Action: U.S. Authorities Disrupt NetWalker Ransomware
https://blog.chainalysis.com/reports/netwalker-ransomware-disruption-arrest/

Attacks targeting healthcare organizations spike globally as COVID-19 cases rise again
https://blog.checkpoint.com/2021/01/05/attacks-targeting-healthcare-organizations-spike-globally-as-covid-19-cases-rise-again/

FBI PIN: Egregor Ransomware Targets Businesses Worldwide, Attempting to Extort Businesses by Publicly Releasing Exfiltrated Data
https://www.documentcloud.org/documents/20444693-fbi-pin-egregor-ransomware-bc-01062021

Microsoft fixes actively exploited Exchange zero-day bugs, patch now
https://www.bleepingcomputer.com/news/security/microsoft-fixes-actively-exploited-exchange-zero-day-bugs-patch-now/

Microsoft Patches Four Zero-Day Exchange Server Bugs
https://www.infosecurity-magazine.com/news/microsoft-patch-four-zeroday/

State hackers rush to exploit unpatched Microsoft Exchange servers
https://www.bleepingcomputer.com/news/security/state-hackers-rush-to-exploit-unpatched-microsoft-exchange-servers/

Microsoft Fixes Exchange Server Zero-Days Exploited in Active Attacks
https://www.darkreading.com/threat-intelligence/microsoft-fixes-exchange-server-zero-days-exploited-in-active-attacks/d/d-id/1340305

More hacking groups join Microsoft Exchange attack frenzy
https://www.bleepingcomputer.com/news/security/more-hacking-groups-join-microsoft-exchange-attack-frenzy/

References

Exchange servers under siege from at least 10 APT groups
https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

Almost 2,000 Exchange servers hacked using ProxyShell exploit
https://therecord.media/almost-2000-exchange-servers-hacked-using-proxyshell-exploit/

Microsoft Exchange servers being hacked by new LockFile ransomware
https://www.bleepingcomputer.com/news/security/microsoft-exchange-servers-being-hacked-by-new-lockfile-ransomware/

Multiple threat actors, including a ransomware gang, exploiting Exchange ProxyShell vulnerabilities
https://doublepulsar.com/multiple-threat-actors-including-a-ransomware-gang-exploiting-exchange-proxyshell-vulnerabilities-c457b1655e9c

ProxyLogon is Just the Tip of the Iceberg
https://i.blackhat.com/USA21/Wednesday-Handouts/us-21-ProxyLogon-Is-Just-The-Tip-Of-The-Iceberg-A-New-Attack-Surface-On-Microsoft-Exchange-Server.pdf

U.S. Government Releases Indictment and Several Advisories Detailing Chinese Cyber Threat Activity
https://us-cert.cisa.gov/ncas/current-activity/2021/07/19/us-government-releases-indictment-and-several-advisories-detailing

REvil ransomware operators claim group is ending activity again, victim leak blog now offline
https://www.zdnet.com/article/revil-ransomware-operators-claim-group-is-ending-activity-again-happy-blog-now-offline/

BlackMatter ransomware gang rises from the ashes of DarkSide, Revil
https://www.bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/

References

Chainalysis in Action: U.S. Authorities Disrupt NetWalker Ransomware
https://blog.chainalysis.com/reports/netwalker-ransomware-disruption-arrest/

HHS outlines threats to electronic health and medical records, remediation guidance
https://www.scmagazine.com/analysis/incident-response/hhs-outlines-threats-to-electronic-health-and-medical-records-remediation-guidance

Kaseya obtains key to decrypt systems weeks after ransomware attack
https://thehill.com/policy/technology/564401-kaseya-obtains-key-to-decrypt-systems-weeks-after-ransomware-attack

19 days after REvil's ransomware attack on Kaseya VSA systems, there's a fix
https://www.theverge.com/2021/7/22/22589643/ransomware-kaseya-vsa-decryptor-revil

Kaseya obtains universal decryptor for REvil ransomware victims
https://www.bleepingcomputer.com/news/security/kaseya-gets-universal-decryptor-for-revil-ransomware-attack-victims/

Kaseya warns of phishing campaign pushing fake security updates
https://www.bleepingcomputer.com/news/security/kaseya-warns-of-phishing-campaign-pushing-fake-security-updates/

REvil victims are refusing to pay after flawed Kaseya ransomware attack
https://www.bleepingcomputer.com/news/security/revil-victims-are-refusing-to-pay-after-flawed-kaseya-ransomware-attack/

Some Kaseya victims privately negotiating with Revil
https://www.databreaches.net/some-kaseya-victims-privately-negotiating-with-revil/

References

Malware campaign targets companies waiting for Kaseya security patch
https://grahamcluley.com/malware-campaign-targets-companies-waiting-for-kaseya-security-patch/

PrintNightmare, Critical Windows Print Spooler Vulnerability
https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/printnightmare-critical-windows-print-spooler-vulnerability

US warns of action against ransomware gangs if Russia refuses
https://www.bleepingcomputer.com/news/security/us-warns-of-action-against-ransomware-gangs-if-russia-refuses/

Coop supermarket closes 500 stores after Kaseya ransomware attack
https://www.bleepingcomputer.com/news/security/coop-supermarket-closes-500-stores-after-kaseya-ransomware-attack/

IBM Cost of a Data Breach Report 2021
https://www.ibm.com/downloads/cas/OJDVQGRY

Putin says Russia would accept conditional handover of cyber criminals to U.S.
https://www.reuters.com/world/putin-says-russia-would-accept-conditional-handover-cyber-criminals-us-2021-06-13/

PoC for critical Windows Print Spooler flaw leaked (CVE-2021-1675)
https://www.helpnetsecurity.com/2021/06/30/poc-cve-2021-1675/

Public Windows PrintNightmare 0-day exploit allows domain takeover
https://www.bleepingcomputer.com/news/security/public-windows-printnightmare-0-day-exploit-allows-domain-takeover/

References

Authorities plan to mass-uninstall Emotet from infected hosts on April 25, 2021
https://www.zdnet.com/google-amp/article/authorities-plan-to-mass-uninstall-emotet-from-infected-hosts-on-march-25-2021/

Emotet Botnet Disrupted in International Cyber Operation
https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation

Cleaning up after Emotet: the law enforcement file
https://blog.malwarebytes.com/threat-analysis/2021/01/cleaning-up-after-emotet-the-law-enforcement-file/

After 7 Years of Reigning Malicious Terror, Emotet's Uninstallation Sets in Motion
https://cisomag.eccouncil.org/after-7-years-of-reigning-malicious-terror-emotets-uninstallation-sets-in-motion/

Last Chance for Forensics Teams Ahead of Emotet Sunday Deadline
https://www.infosecurity-magazine.com/news/last-chance-forensics-teams-emotet/

Cyberattack disrupts Colonial Pipeline, which transports 100 million gallons of fuel daily
https://www.cyberscoop.com/gas-pipeline-cyberattack-ransomware-colonial/

Colonial Pipeline Confirms Ransomware Causing Disruptions
https://www.healthcareinfosecurity.com/colonial-pipeline-confirms-ransomware-causing-disruptions-a-16549

Media Statement Update: Colonial Pipeline System Disruption
https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption

Cyberattack disrupts Colonial Pipeline, which transports 100 million gallons of fuel daily
https://www.cyberscoop.com/gas-pipeline-cyberattack-ransomware-colonial/

Colonial Pipeline Confirms Ransomware Causing Disruptions
https://www.healthcareinfosecurity.com/colonial-pipeline-confirms-ransomware-causing-disruptions-a-16549

References

Why international efforts were needed to tackle EMOTET (Includes interview)
https://www.digitaljournal.com/tech-science/why-international-efforts-were-needed-to-tackle-emotet/article/588822

Colonial Pipeline reports data breach after May ransomware attack
https://www.bleepingcomputer.com/news/security/colonial-pipeline-reports-data-breach-after-may-ransomware-attack/

Media Statement Update: Colonial Pipeline System Disruption
https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption

Executive Order on Improving the Nation's Cybersecurity
https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

FACT SHEET: President Signs Executive Order Charting New Course to Improve the Nation's Cybersecurity and Protect Federal Government Networks
https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/12/fact-sheet-president-signs-executive-order-charting-new-course-to-improve-the-nations-cybersecurity-and-protect-federal-government-networks/

Biden signs much-anticipated cybersecurity executive order
https://fcw.com/articles/2021/05/12/cyber-executive-order.aspx

'Number of days' before systems back working – HSE
https://www.rte.ie/news/health/2021/0514/1221519-hospital-it-problem/

Universities Across the Country Are Being Swept Up in a Large Data Fiasco
https://gizmodo.com/universities-across-the-country-are-being-swept-up-in-a-1846602529

References

Biden signs executive order to improve federal cybersecurity
https://thehill.com/policy/cybersecurity/553243-biden-signs-executive-order-to-improve-federal-cybersecurity-following

Ireland's national health service offers sitrep after ransomware attack knocked systems offline
https://portswigger.net/daily-swig/irelands-national-health-service-offers-sitrep-after-ransomware-attack-knocked-systems-offline

HSE Can't Guarantee That Health Information Won't Be Published Online
https://www.spinsouthwest.com/news-and-sport/hse-cant-guarantee-that-health-information-wont-be-published-online-1196075

Hospitals and Health Systems Warned of Elevated Risk of Destructive Cyberattacks
https://www.hipaajournal.com/hospitals-and-health-systems-warned-of-elevated-risk-of-destructive-cyberattacks/

Iran's hackers are using these tools to steal passwords and deliver ransomware, say FBI and CISA
https://www.zdnet.com/article/irans-hackers-are-using-these-tools-to-steal-passwords-and-deliver-ransomware-say-fbi-and-cisa/

Conti ransomware also targeted Ireland's Department of Health
https://www.bleepingcomputer.com/news/security/conti-ransomware-also-targeted-irelands-department-of-health/

A New Attack Surface on MS Exchange Part 2 - ProxyOracle!
https://blog.orange.tw/2021/08/proxyoracle-a-new-attack-surface-on-ms-exchange-part-2.html

Chinese Hacking Spree Hit an 'Astronomical' Number of Victims
https://www.wired.com/story/china-microsoft-exchange-server-hack-victims/

References

Stanford, University Of California Targeted In Widespread Ransomware Cyber Attack
https://sanfrancisco.cbslocal.com/2021/04/03/stanford-university-of-california-targeted-in-widespread-ransomware-cyber-attack/

UC Berkeley confirms data breach, becomes latest victim of Accellion cyber-attack
https://portswigger.net/daily-swig/uc-berkeley-confirms-data-breach-becomes-latest-victim-of-accellion-cyber-attack

BlackKingdom ransomware still exploiting insecure Exchange servers
https://nakedsecurity.sophos.com/2021/03/23/blackkingdom-ransomware-still-exploiting-insecure-exchange-servers/

Microsoft: Black Kingdom ransomware group hacked 1.5K Exchange servers
https://www.bleepingcomputer.com/news/security/microsoft-black-kingdom-ransomware-group-hacked-15k-exchange-servers/

Analyzing attacks taking advantage of the Exchange Server vulnerabilities
https://www.microsoft.com/security/blog/2021/03/25/analyzing-attacks-taking-advantage-of-the-exchange-server-vulnerabilities/

GitHub: microsoft/CSS-Exchange
https://github.com/microsoft/CSS-Exchange/blob/main/Security/src/http-vuln-cve2021-26855.nse

At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software
https://krebsonsecurity.com/2021/03/at-least-30000-u-s-organizations-newly-hacked-via-holes-in-microsofts-email-software/

A Basic Timeline of the Exchange Mass-Hack
https://krebsonsecurity.com/2021/03/a-basic-timeline-of-the-exchange-mass-hack/

References

This new Microsoft tool checks Exchange Servers for ProxyLogon hacks
https://www.bleepingcomputer.com/news/microsoft/this-new-microsoft-tool-checks-exchange-servers-for-proxylogon-hacks/

Microsoft IOC Detection Tool for Exchange Server Vulnerabilities
https://us-cert.cisa.gov/ncas/current-activity/2021/03/06/microsoft-ioc-detection-tool-exchange-server-vulnerabilities

China-Linked Hack Hits Tens of Thousands of U.S. Microsoft Customers
https://www.wsj.com/articles/china-linked-hack-hits-tens-of-thousands-of-u-s-microsoft-customers-11615007991

Move over, SolarWinds: 30,000 orgs' email hacked via Microsoft Exchange Server flaws
https://www.theverge.com/2021/3/5/22316189/microsoft-exchange-server-security-exploit-china-attack-30000-organizations

Microsoft Releases Alternative Mitigations for Exchange Server Vulnerabilities
https://us-cert.cisa.gov/ncas/current-activity/2021/03/05/microsoft-releases-alternative-mitigations-exchange-server

The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of China
https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/

TrickBot malware dev extradited to U.S. faces 60 years in prison
https://www.bleepingcomputer.com/news/security/trickbot-malware-dev-extradited-to-us-faces-60-years-in-prison/

References

Microsoft Attack Blamed on China Morphs Into Global Crisis
https://www.bloomberg.com/news/articles/2021-03-07/hackers-breach-thousands-of-microsoft-customers-around-the-world

Microsoft's MSERT tool now finds web shells from Exchange Server attacks
https://www.bleepingcomputer.com/news/security/microsofts-msert-tool-now-finds-web-shells-from-exchange-server-attacks/

White House announces ransomware task force — and hacking back is one option
https://www.politico.com/news/2021/07/14/white-house-ransomware-task-force-499723

U.S. Government sets up ransomware task force, offers $10 million reward for info
https://www.helpnetsecurity.com/2021/07/16/ransomware-task-force/

Biden Administration announces flurry of new anti-ransomware efforts
https://www.csoonline.com/article/3625672/biden-administration-announces-flurry-of-new-anti-ransomware-efforts.html

U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov
https://www.justice.gov/opa/pr/us-government-launches-first-one-stop-ransomware-resource-stopransomwaregov

Rewards for Justice – Reward Offer for Information on Foreign Malicious Cyber Activity Against U.S. Critical Infrastructure
https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-foreign-malicious-cyber-activity-against-u-s-critical-infrastructure/

Reproducing The ProxyShell Pwn2Own Exploit
https://peterjson.medium.com/reproducing-the-proxyshell-pwn2own-exploit-49743a4ea9a1

REvil ransomware shuts down again after Tor sites were hijacked
https://www.bleepingcomputer.com/news/security/revil-ransomware-shuts-down-again-after-tor-sites-were-hijacked/

Man gets 7 years in prison for hacking 65K health care employees
https://www.bleepingcomputer.com/news/security/man-gets-7-years-in-prison-for-hacking-65k-health-care-employees/

US links $5.2 billion worth of Bitcoin transactions to ransomware
https://www.bleepingcomputer.com/news/security/us-links-52-billion-worth-of-bitcoin-transactions-to-ransomware/

FinCEN: Financial Trend Analysis - Ransomware Trends in Bank Secrecy Act Data Betweeen January 2021 and June 2021
https://www.fincen.gov/sites/default/files/shared/Financial%20Trend%20Analysis_Ransomeware%20508%20FINAL.pdf

Cyberattack on Alabama hospital linked to 1st alleged ransomware death
https://www.beckershospitalreview.com/cybersecurity/cyberattack-on-alabama-hospital-linked-to-1st-alleged-ransomware-death.html

Microsoft Exchange servers scanned for ProxyShell vulnerability, Patch Now
https://www.bleepingcomputer.com/news/microsoft/microsoft-exchange-servers-scanned-for-proxyshell-vulnerability-patch-now/

TrickBot gang developer arrested when trying to leave Korea
https://www.bleepingcomputer.com/news/security/trickbot-gang-developer-arrested-when-trying-to-leave-korea/

Questions

Upcoming Briefs

- 3/17 – Analysis of the Potential Russian Cyberthreat to the U.S. Health Sector

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV**.

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback, please complete the HC3 Customer Feedback Survey.

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Direct communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG.

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic, or want to join our Listserv? Send your request for information (RFI) to HC3@HHS.GOV,or visit us at www.HHS.Gov/HC3.

Contact

www.HHS.GOV/HC3

HC3@HHS.GOV