2021

Cyber security threat trends:

phishing, crypto top the list

The bridge to possible

Introduction

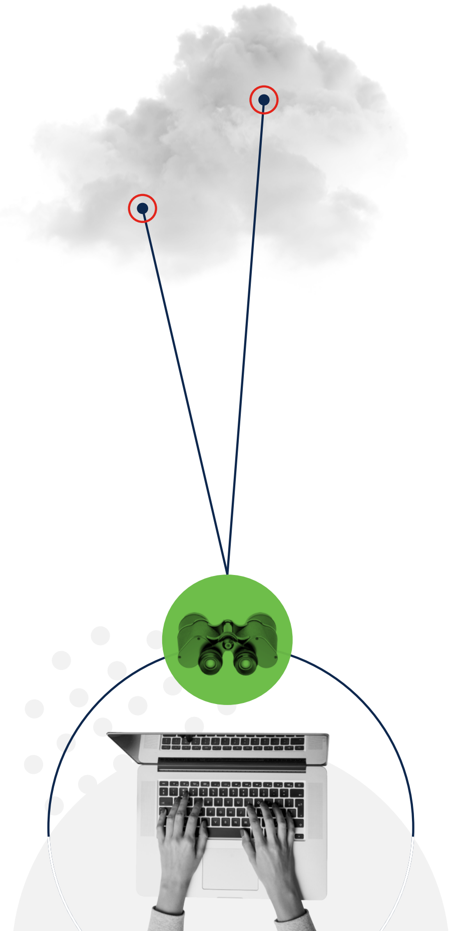
When you serve as the internet's switchboard, you see a lot of hookups. Cisco Umbrella's cloud-native global cloud architecture processes more than 620 billion internet requests daily. Often times, it's the relationships between different types of active threats and the associated internet activity directed toward malicious domains that deliver deeper insights into patterns of cybercriminal behavior.

The data in this report reflects a continuation of the trend we have been seeing toward more complex, multi-staged attacks that involve multiple threat types. Typically, in the attack chain, we're seeing things like a trojan begat an information loader, which begat a ransomware demand.

As we noted in The modern cybersecurity landscape: Scaling for threats in motion, for cybercrime, "the goal is to insert proven attack elements like Emotet and Ursnif/Gozi to reduce risk and new coding efforts, while focusing on the orchestrated movements that will hide the attackers' full intent."

We've examined the threats that were most active in 2020[1] and here are some of the insights we've uncovered. The charts associated with these insights focus on two metrics: the number of endpoints alerting to malicious activity (depicted by line graphs in the following charts), and the amount of internet query (DNS) traffic seen for each type of threat (shown by bar graphs in the charts). We're reporting on data for the calendar year 2020.

Here are some of the highlights from this report:

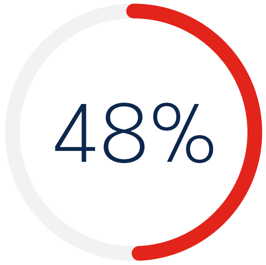


of organizations had at least one user try to connect to a phishing site

of organizations had users that were served malicious browser ads

of organizations experienced some level of unsolicited cryptomining

of organizations encountered ransomware-related activity



found information-stealing malware activity

Overall, cryptomining, phishing, ransomware, and trojans averaged 10x the internet activity of all other threat types

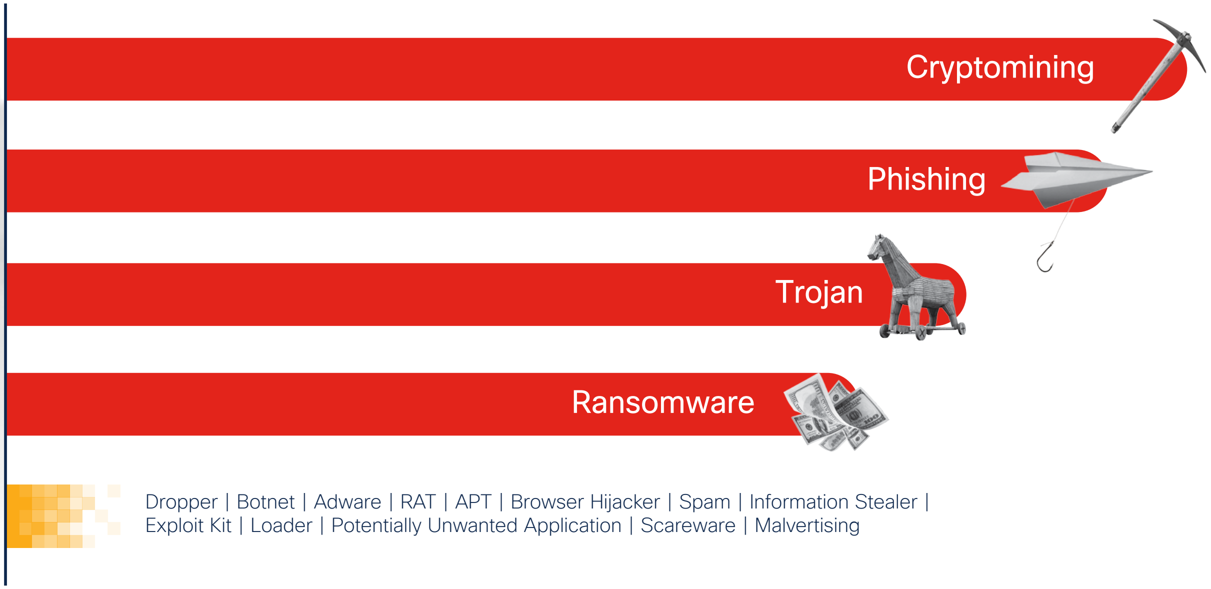
INSIGHT 1

Cryptomining, phishing, ransomware, and trojans are the most active threats

These four threat types averaged internet query volumes of around 100 million each month, whereas the next dozen threat types hovered around 10% of that. As we noted at the beginning, there is some relationship between these most frequently seen threat types – particularly between phishing, trojans, and ransomware. More about this further in the report.

10x

more queries than all other threat types



INSIGHT 2

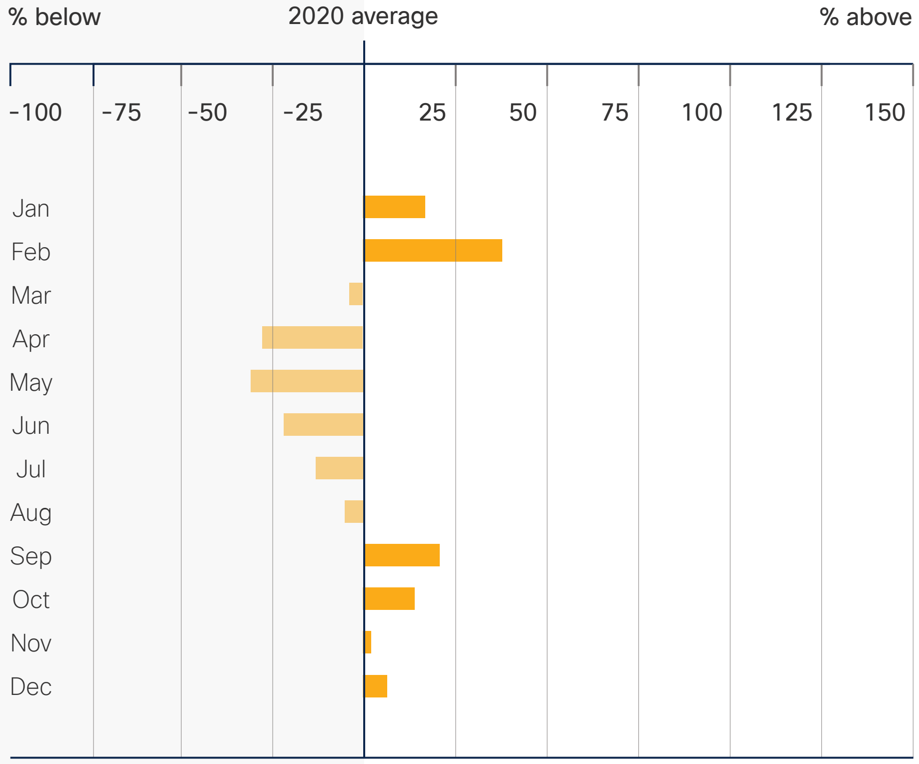
Cryptomining generated the most internet traffic out of any individual category

We found that 69% of organizations experienced some level (at least one end-user instance) of unsolicited cryptomining. It's not surprising that cryptomining generated the most internet traffic out of any individual category. While cryptomining is often favored by bad actors for low-key revenue generation, it's relatively noisy on the DNS side, as it regularly pings mining servers for more work.

Cryptomining, when software-based, often serves as a gateway into more serious forms of cybercrime. Malicious third parties get into your environment, and then set up a miner to make passive income while they conduct lateral moves to exfiltrate data or do something else malicious.

Organizational impact depends on the extent of mining happening in that environment. At its most basic level, cryptomining can reduce the life of your hardware, clog your bandwidth, and drive up your AWS compute costs depending on how the miner has been configured. In the worst-case scenario, a malicious actor infiltrated your environment and setup a miner to make passive income while the peruse your environment for data to exfiltrate or to exploit your environment further with follow-up malware. Bottom-line, if you see a lot of cryptomining traffic you should investigate to avoid a potential IOC.

In 2020, cryptomining was most active early in the year. It declined until summer, then gradually recovered in the later part of the year. As currency values increased, so too did the rate of activity, particularly when looking at associated endpoint queries.



3

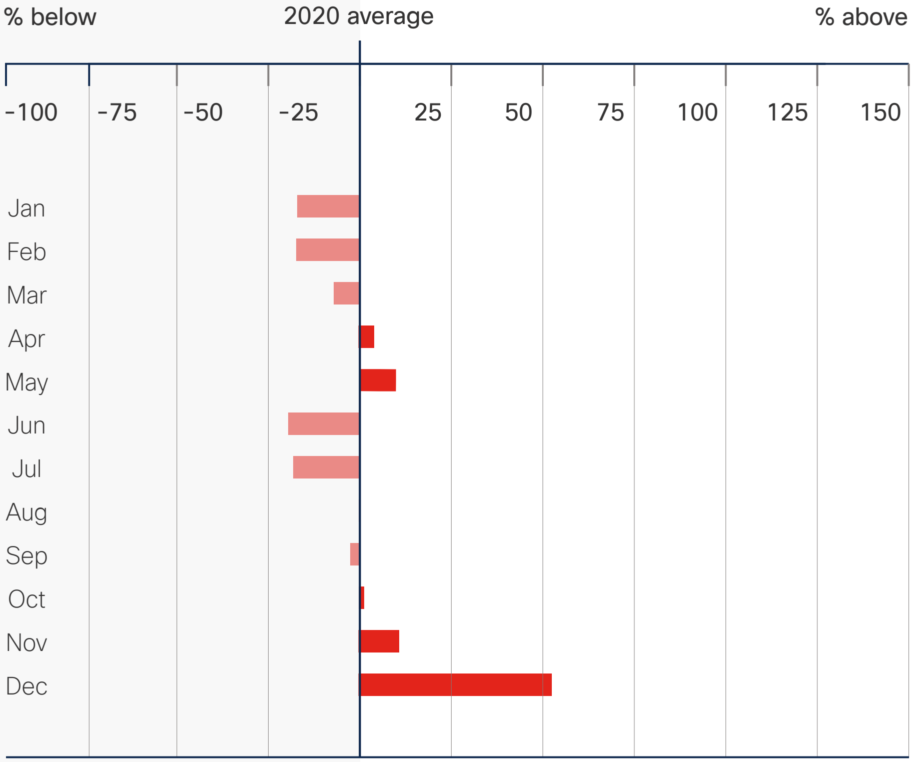
INSIGHT 3

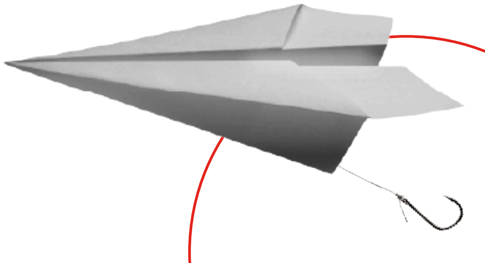
Phishing mostly stable with some surprises

Phishing, though an old tactic, continues to be popular due to its simplicity and effectiveness. It targets the weakest link in the security chain: the user. Phishers usually masquerade as a trustworthy entity in an electronic communication. That's probably why it accounts for 90% (that's not a typo) of data breaches.

We have seen a notable uptick in overall phishing activity and the pandemic in part drove that spike. The pandemic has us thirsty for information (e.g., free testing sites, vaccine signups sites, etc.) and malicious actors have jumped at the opportunity to setup numerous credential phishing and malware dropper sites. Most of these sites mimic content from the CDC, ECDC, or other health and government authorities. Looking at our telemetry, North America and EMEA accounted for 77% of the malicious pandemic traffic we saw in 2020.

Phishing was fairly stable in 2020, with the exception of December, which saw a 52% increase around the holidays. In terms of the number of endpoints visiting phishing sites, there were significant increases during August and September, due to a very large phishing campaign, where we see a 102% shift between July and September.





INSIGHT 4

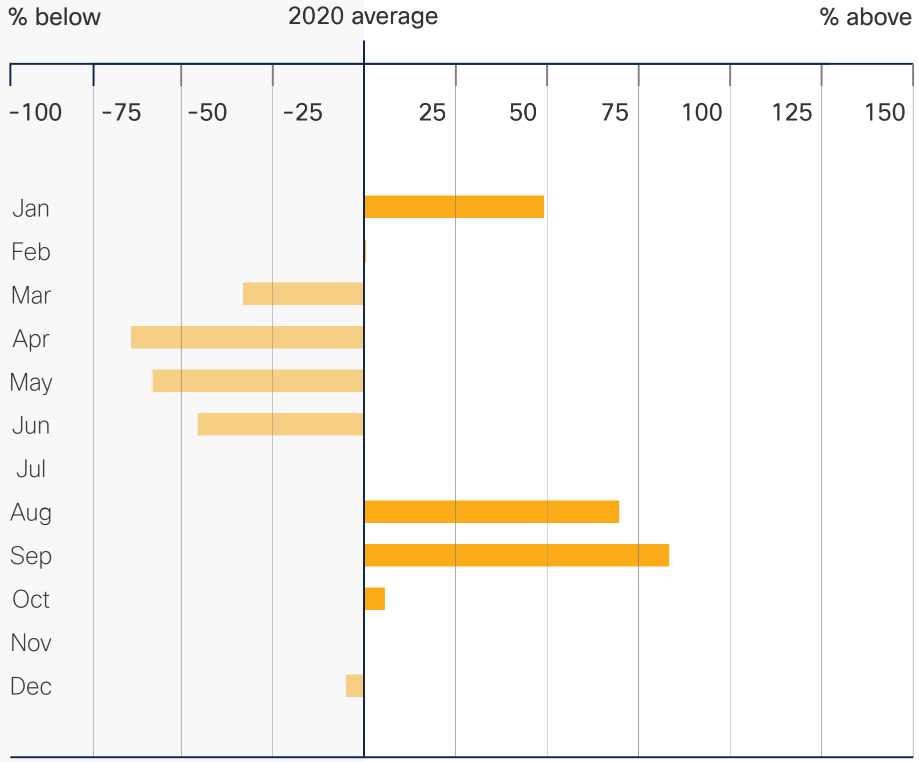
Ursnif/Gozi and IcedID drive early year trojan numbers

Trojans started the year strong. The incredibly high number of endpoints connecting to trojan sites was largely due to Ursnif/Gozi and IcedID—two threats known to work in tandem to deliver ransomware. These two threats alone comprised 82% of trojans seen on endpoints in January.

In late July, Emotet emerged from its slumber once again, comprising a massive amount of traffic that grew through September. This threat alone is responsible for the large increase in internet query activity from August through September. In all, 45% of organizations encountered Emotet.

In all, the trojan data we observed in 2020 continues a trend of trojans gaining a second life for new forms of malware delivery. Emotet is a good example of this, having started as a successful banking trojan, but quickly evolving into an even more successful malware dropper.

Ursnif/Gozi is another example of a trojan/dropper that is evolving its use cases. It leverages email thread hijacking and abuse of trusted services such as Google Drive. Its targeted approach to the choice of delivery method depending on potential victims has made it popular in a wide variety of attacks. due to a very large phishing campaign, where we see a 102% shift between July and September.



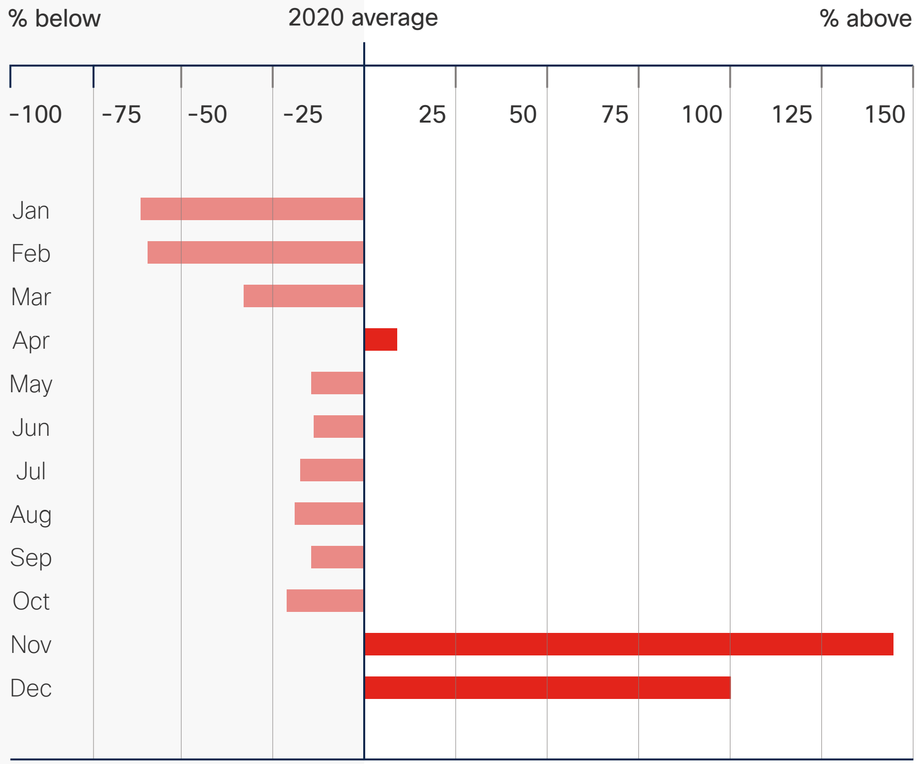
INSIGHT 5

Sodinokibi and Ryuk tell tale of 2 ransomware threats in 2020

Ransomware in 2020 was bookended by two different threats: Sodinokibi and Ryuk. Sodinokibi, which hits a lot of endpoints because of the relatively small ransoms demanded, drove up query volumes in September. Ryuk, which affects fewer endpoints but demands higher ransoms, finished up the year in December with internet query volumes so high that it skewed the entire category for 2020.

Most of the domains associated with Ryuk activity are command-and-control (C&C) domains. These types of domains usually generate significant amounts of queries. Infected computers where actors got initial access but didn't deploy ransomware consistently check in with multiple C&C servers to make sure it stays available for further exploitation.

Ryuk was particularly a problem for the healthcare, financial services, and higher education industry segments, in order of severity. Those high query volumes displayed in November and December in the chart are almost exclusively affecting healthcare and financial services firms.



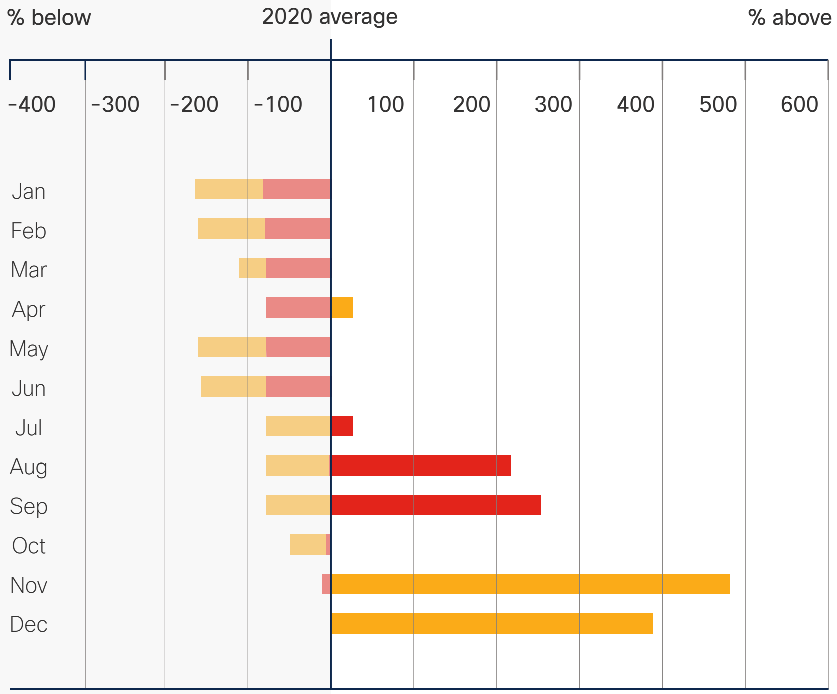
INSIGHT 6

Phishing delivers Emotet to deploy Ryuk

The most prevalent attacks these days leverage a variety of threats at different stages. If threats had social media profiles, for Phishing, Emotet, and Ryuk, the relationship statuses would have to be “It’s complicated.” Remember the 102% shift in phishing between July and September? This lines up with a 216% jump in Emotet internet query activity. Activity drops off in October, followed by an eye-watering 480% increase in Ryuk activity.

Most of the domains associated with Ryuk activity are command-and-control (C&C) domains. These types of domains usually generate significant amounts of queries. Infected devices where actors got initial access but didn’t deploy ransomware consistently check in with multiple C&C servers to make sure it stays available for further exploitation.

Turning next to a few key industry segments, we’ll look at how some of these top threats are affecting organizations in financial services, healthcare, and manufacturing.

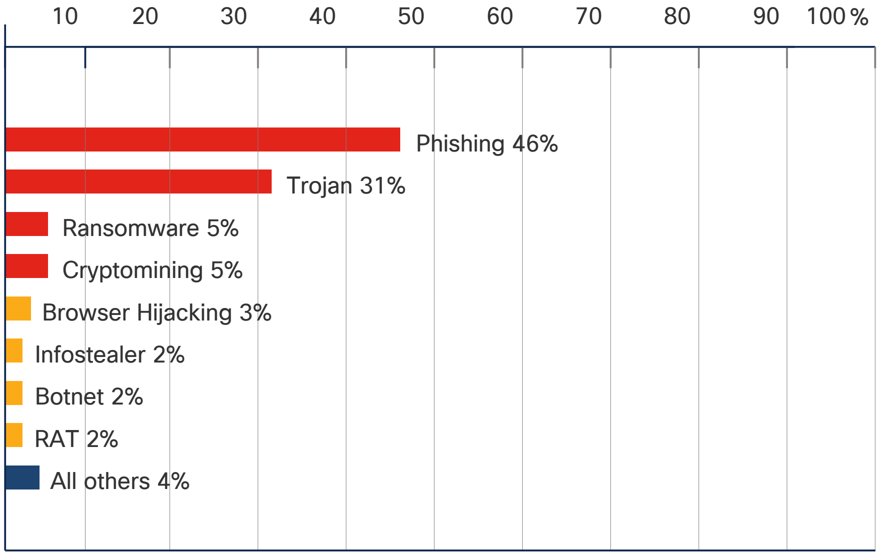


INSIGHT 7

Cyber criminals phish FSIs for information that pays off

Phishing resulted in the highest levels of malicious query traffic in the financial services sector. It also dominated all other industries in this category. In fact, this sector saw 60% more phishing than the next-closest sector, higher education. It's possible that this sector is targeted by attackers through phishing more often than others simply because of its proximity to many bad actor's end goal: money.

Supporting this theory is the fact that the financial services sector also saw more information-stealing threats than any other industry. While not known to generate high volumes of internet query traffic (only 2%), financial services saw five times as much traffic in this category than any other industry. healthcare, and manufacturing.



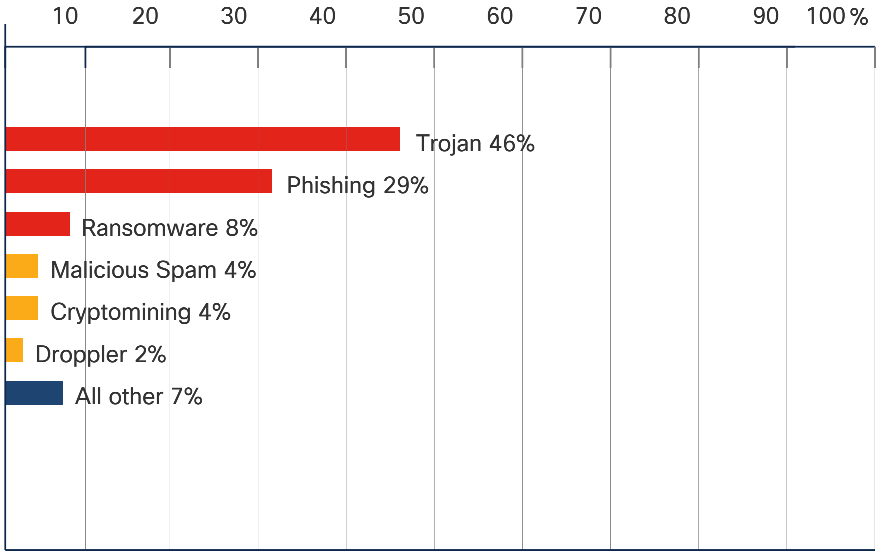
INSIGHT 8

Healthcare sees higher trojan, phishing, ransomware activity

In a reverse from the financial services industry, the healthcare industry saw trojan activity first and phishing activity second. These two together made up three quarters of malicious traffic in this industry.

The healthcare industry saw more trojans than any other sector, as well as higher numbers of droppers. It was also narrowly edged out of the second-highest place for ransomware, coming in only 1.5% lower in overall number of internet queries.

As mentioned earlier, the massive spike in Ryuk internet queries came particularly at the expense of healthcare organizations, likely reflecting some big game hunting among cyber attackers.

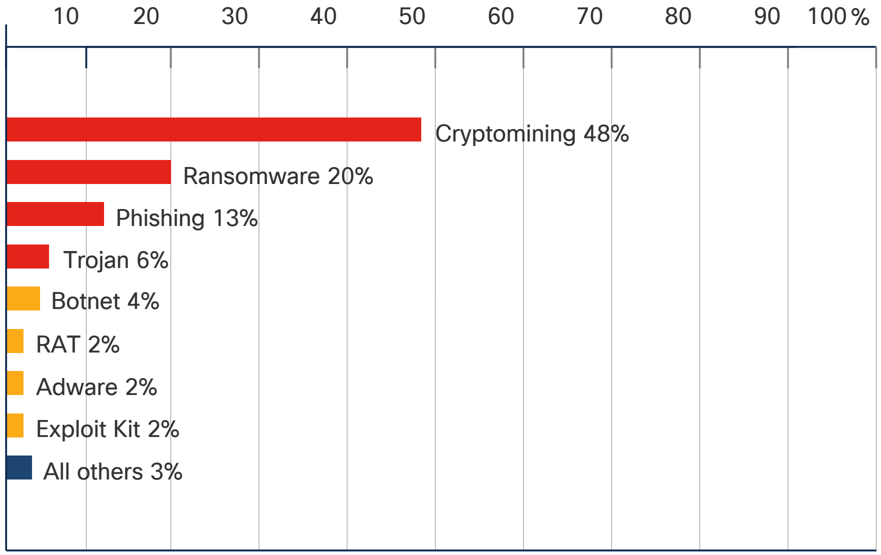


INSIGHT 9

Ransomware bedevils manufacturing endpoints more than other industries

Like the technology sector, cryptomining activity was also high in the manufacturing industry. It saw roughly half the activity seen in the technology sector, but interestingly, there were almost three times as many endpoints in the manufacturing sector involved in cryptomining. In short, more machines resulting in less internet queries leads us to believe these endpoints were less powerful when compared to those in the technology sector. It's possible that the machines compromised are involved in the manufacturing process itself, even IoT related. In these cases, cryptomining would likely have been slower, but could still impact production speeds.

It turns out that the manufacturing sector is also the most likely to be impacted by ransomware. This industry saw almost as much ransomware-related traffic as the next two closest industries combined (technology and healthcare). This appears to be a clear indication the industry is regularly targeted by bad actors, likely due to the damage that big game hunting can wreak, and the potential payout bad actors could receive.



Summary

If you find one threat within your network, it's wise to investigate what threats are working in tandem with it and take precautionary measures to prevent them from causing further havoc.

The data used in this report comes from Cisco Umbrella, our cloud delivered security service that includes DNS-layer security, secure web gateway, firewall, cloud access security broker (CASB) functionality, and threat intelligence. In each of these cases, the malicious activity was stopped in its tracks by Umbrella. The user who clicked on a phishing email was unable to connect to the malicious site. The RAT attempting to talk to its C2 server was unable to phone home. The illicit cryptominer couldn't get work to mine for cryptocurrency.

Using our massive and diverse dataset – collected across more than 620 billion internet requests from across 190 countries and further enriched with data from both private feeds and a handful of public ones – our world-class team of engineers, mathematicians, and security researchers can uncover patterns that signal malicious behavior. This analysis is based on aggregated DNS query logs paired with scrubbed and anonymized customer demographic information. Together, they give us a unique perspective on global DNS traffic, which helps us both see the trends and defend against them.

Cisco Umbrella protects against more than 7 million malicious domains and IPs, while discovering over 60,000 new malicious destinations (domains, IPs, and URLs) every day. Each node of attack infrastructure is an opportunity to identify and neutralize threat architecture before it can be used for new attacks.

Umbrella combines multiple security functions into one solution, so you can extend protection to devices, remote users, and distributed locations anywhere. Umbrella is the easiest way to effectively protect your users everywhere in minutes.

Also, if you're looking to get more information on the malicious domains that your organization encounters, Umbrella Investigate gives the most complete view of the relationships and evolution of internet domains, IPs, and files – helping to pinpoint attackers' infrastructures and predict future threats. No other vendor offers the same level of interactive threat intelligence – exposing current and developing threats. Umbrella delivers the context you need for faster incident investigation and response.

Glossary

We refer to threat types in the charts and text of this report. Cisco Umbrella uses three levels of classification to illustrate the relationships between the broader categories and types of threats. Threat types form the middle tier, comprising groups of specific threats, such as Ryuk or IcedID. The former is an example of a ransomware threat and the latter, IcedID, is an example of a trojan.

Adware: Adware, or advertising-supported software, is any software package that automatically renders advertisements in order to generate revenue for the author. The advertisements may be in the user interface of the software or presented in the web browser. Adware may cause tabs to open automatically that display advertising, make changes to the home page settings in your web browser, offer ad-supported links from search engines, or initiate redirects to advertising websites.

APT: An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by cyber criminals targeting a specific entity. An APT usually targets organizations and/or nations for business or political motives.

Backdoor: A backdoor is a type of trojan that enables threat actors to gain remote access and control over a system. The backdoor is often the final stage in gaining full control over a system.

Botnet: A botnet is a number of internet-connected systems infected with malware that communicate and coordinate their actions received from command and control (C&C) servers. The infected systems are referred to as bots. The most typical uses of botnets are DDoS attacks on selected targets and the propagation of spam.

Browser hijacker: A browser hijacker is any malicious code that modifies a web browser's settings without a user's permission, to inject unwanted advertising into the user's browser or redirect to fraudulent or malicious sites. It may replace the existing home page, error page, or search page with its own. It can also redirect web requests to unwanted destinations.

Bulletproof hosting: Bulletproof hosting is a service provided by some domain hosting or web hosting firms that allows their customer considerable leniency in the kinds of material they may upload and distribute. This type of hosting is often used for spamming, phishing, and other illegal cyber activities.

Cryptojacking: Cryptojacking is malicious cryptomining and the covert use of a systems computer resources to mine cryptocurrency. Cryptojacking is initiated by malware or through web cryptominers embedded in website code.

Drive-by download: A drive-by download is any download that happens without a person's consent or knowledge.

Dropper: A dropper is a program or malware component that has been designed to "install" some sort of malware (ransomware, backdoor, etc.) to a target system. The dropper may download the malware to the target machine once it is received from the command-and-control server or from other remote locations.

Exploit kit: An exploit kit is a software kit designed to run on web servers with the purpose of identifying software vulnerabilities in client machines communicating with it and discovering and exploiting vulnerabilities to upload and execute malicious code on the client.

Fast flux botnet: Fast flux is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies. It can also refer to the combination of peer-to-peer networking, distributed command and control, web-based load balancing and proxy redirection used to make malware networks more resistant to discovery and counter-measures.

Information stealer: An information stealer is a trojan that can harvest keystrokes, screenshots, network activity, and other information from systems where it is installed. It may also covertly monitor user behavior and harvest personally identifiable information (PII) including names and passwords, chat programs, websites visited, and financial activity. It may also be capable of covertly collecting screenshots, video recordings, or have the ability to activate any connected camera or microphone. Collected information may be stored locally and later retrieved, or may be transmitted to a command-and-control server.

Loader: A loader is a type of malware or malicious code used in the loading of a second-stage malware payload onto a victim's system. The loader is able to hide a malware payload inside the actual loader code instead of contacting a remote location to download a second-stage payload.

Malvertising: Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages. Malvertising is often used in exploit kit redirection campaigns.

Mobile trojan: A mobile trojan is a trojan designed to target and infect mobile phones running Android, iOS, Windows or other mobile operating systems.

Point-of-sale malware: Point-of-sale malware (POS malware) is used by cybercriminals to target point of sale terminals with the intent to obtain credit card and debit card information by reading the device memory from the retail checkout point of sale system.

Ransomware: Ransomware is computer malware that installs covertly on a victim's computer, encrypts files, and demands a ransom be paid to decrypt the files or to prevent the attacker from publishing the victim's data publicly.

Remote access trojan (RAT): A remote access trojan (RAT) is malware that allows covert surveillance or unauthorized access to a compromised system. RATs make use of specially configured communication protocols. The actions performed vary but follow typical trojan techniques of monitoring user behavior, exfiltrating data, lateral movement, and more.

Rootkit: A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorized user) and often masks its existence or the existence of other software.

Scareware: Scareware is a form of malicious software or website that uses social engineering to give the perception of a threat in order to manipulate users into buying or installing unwanted software. Scareware misleads users by using fake alerts to trick them into believing there is malware on their computer, and manipulates them into paying money for a fake malware removal tool or allowing an entity remote access to their system to clean the malware. Instead of remediation, the software or remote entity delivers malware to the computer.

Sinkhole: A DNS sinkhole, also known as a sinkhole server, is a DNS server that gives out false information, to prevent the use of the domain names it represents. Traffic is redirected away from its intended target. DNS sinkholes are often used to disrupt botnet command and control servers.

Spam: Spam is an unwanted, unsolicited message that can be received through email or SMS texts. Spam is sent to many users in bulk. It is often sent through the means of a botnet. Spam can contain advertising, scams, or soliciting. In the case of malspam or malicious spam, it contains malicious attachments or links that lead to malware.

Spyware: Spyware gathers information about a person or organization without their knowledge. It may assert control over a computer without the user's knowledge.

Trojan: A trojan is malware which is used to compromise a system by misleading users of its true intent. Trojans typically create a backdoor, exfiltrate personal information, and can deliver additional malicious payloads.

Worm: A computer worm is malware that replicates itself in order to spread to other computers. Worms typically spread through the computer network or removable storage devices that are shared between systems, relying on security failures on the target computer.

About Cisco Umbrella

Cisco Umbrella's cloud-native infrastructure scales to process billions of DNS requests per day, representing 24K+ enterprise customers from 190+ countries – and rising. By unifying multiple security solutions into a single service, Cisco Umbrella helps businesses embrace direct internet access, secure cloud applications, and extend protection to roaming users and branch offices.

Want to learn more?

Check out https://umbrella.cisco.com/ for more details. Or better yet, get started today with a free 14-day trial.

04/21