WHITE PAPER

Ransomware, the Exploding Cyber Threat

A Look at What, Why, and How

Executive Summary

When a cyber threat grows in magnitude by 35 times in one year, and continues to become even more prevalent the next, every organization should pay attention. This is exactly what happened with ransomware. Cyber criminals have targeted organizations from many different industry segments, as well as businesses of virtually every size.

Ransomware-as-a-Service (RaaS) and other kit-like tools have lowered the entry bar for cyber criminals, enabling even novice attackers to be successful against scattered security infrastructures. And monetary technologies like bitcoin make it virtually impossible for law enforcement authorities to track ransom payments. With the exponential growth in ransom paid to ransomware groups, the prospect that this will continue—and at a faster rate—in coming years is great. Recognizing the growing threat, banks are stocking up on bitcoin so their customers can quickly pay cyber criminals to unlock hacked data.

"Over the last year or so, we've really seen an explosion of ransomware and we've seen the ransom demands increasing from tens of thousands of dollars in 2015 to hundreds of thousands of dollars and most recently we've seen ransom demands in the order of millions of dollars."[1]

The Runaway Ransomware Threat

FortiGuard Labs analysis of global data showed a substantial increase in overall ransomware activity in the second half of 2020, compared to the first half. In fact, FortiGuard Labs analyzed the activity for all signatures that it has classified as ransomware, which showed a sevenfold increase in ransomware activity in December compared to July 2020 (see Figure 1).

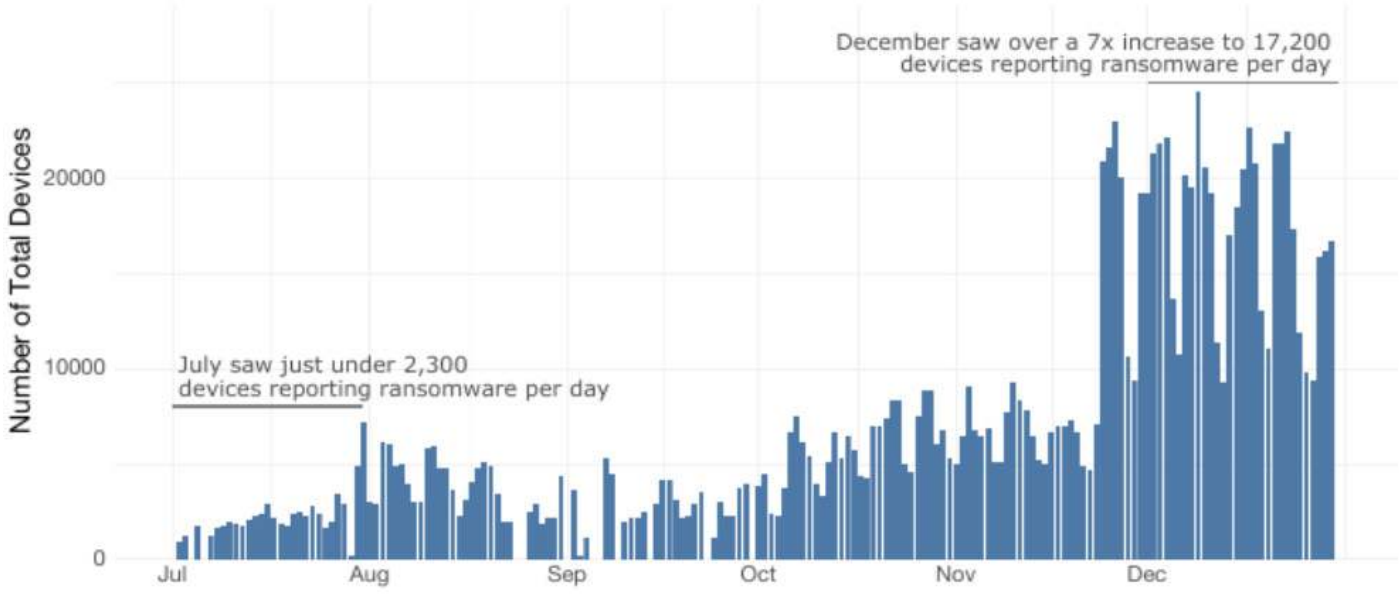


Figure 1: Daily number of devices detecting ransomware variants in 2H 2020.

Among the most active of the ransomware strains in the second half of 2020 were Egregor, Ryuk, Conti, Thanos, Ragnar, WastedLocker, Phobos/EKING, and BazarLoader. Each of these exhibited varying degrees of prevalence, but the common trend among them was an increase in activity over the period (see Figure 2).

Threat actors have discovered that cryptolocking critical systems and demanding a ransom for the decryption key is a relatively easy way to extort money from organizations regardless of size or the industry to which they belong. This more targeted and sinister form of ransomware scheme has come to be known as "big game hunting." It's been all the rage with the ransomware gangs throughout 2020, and the larger paydays netted by such schemes virtually ensure the trend won't go away anytime soon.

Many adversaries took advantage of the disruptions caused by the COVID-19 pandemic to ramp up ransomware attacks against organizations in the healthcare sector in particular. In October, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services, and the FBI issued a joint advisory warning U.S. hospitals and healthcare services of increased ransomware activity involving TrickBot and BazarLoader malware. Other sectors that were also heavily targeted in ransomware attacks in 2H 2020 included professional services firms, consumer services companies, public sector organizations, and financial services firms.

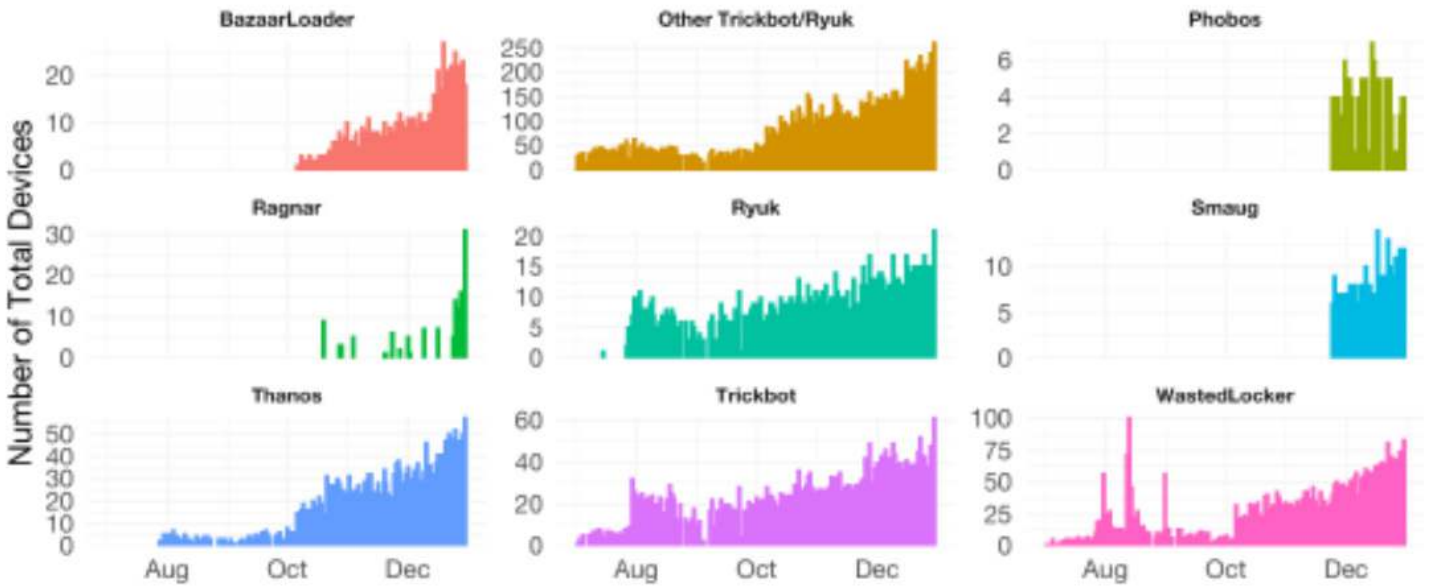


Figure 2: Daily detections of select ransomware strains of interest in 2H 2020.

Multiple trends characterized the ransomware activity that FortiGuard Labs and others observed in the last half of 2020. One of the most troubling was the steady increase in ransomware attacks that involved data exfiltration and the subsequent threat to release the data if a ransom was not paid. The use of data theft as additional leverage in ransomware campaigns really only emerged as an adversary tactic in early 2020, but became part of a majority of attacks by the end of the year.

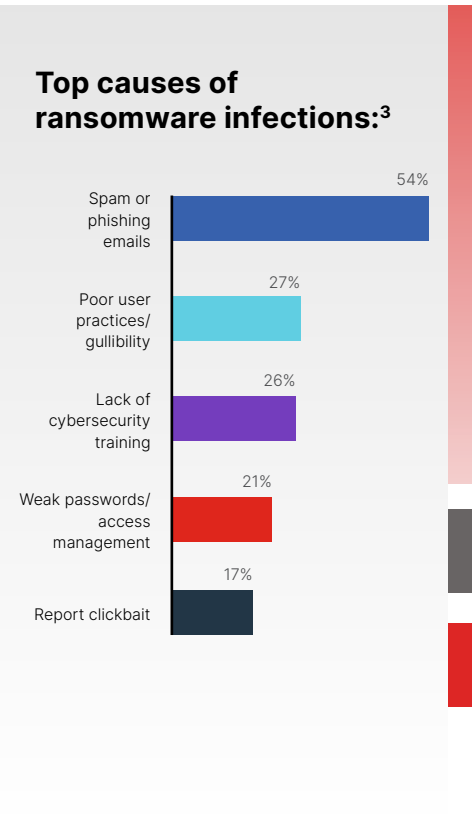
The operators of most major ransomware strains, including Sodinokibi, Ryuk, Egregor, and Conti, all deployed data exfiltration as part of their standard operations last year. Some reported incidents were attacker (sometimes false) claims of data theft to try and scare victims into paying a ransom. In many cases, when victims paid to get attackers to delete stolen data, the attackers reneged and instead leaked or sold the data to others anyway. For organizations, the trend means that robust data backups alone are no longer enough protection against ransomware demands.[2]

How Ransomware Happens

Distribution of Ransomware

So, how does ransomware happen? Let's begin by addressing how it is distributed. Any digital means can be used: email, website attachments, business applications, social media, and USB drivers, among other digital delivery mechanisms. Email remains the number one delivery vector, with cyber criminals preferring to use links first and attachments second.

In the case of email, phishing emails are sent as delivery notifications or fake requests for software updates. Once a user clicks on the link or the attachment, there is often (but less so recently) a transparent download of additional malicious components that then encrypt files with RSA 2048-bit private-key encryption, leaving it nearly impossible for the user to decrypt the files. In other instances, ransomware is embedded as a file on a website, which when downloaded and installed, activates the attack.



Types of Ransomware

Ransomware attacks come in different forms. This past year has seen a substantial evolution in ransomware attacks. Traditional ransomware goes after data, locking files until the ransom is paid. But as mentioned above, with the rapid growth in Internet-of-Things (IoT) devices, a new strain of ransomware emerged. It doesn't go after an organization's data, but targets control systems (e.g., vehicles, manufacturing assembly lines, power systems) and shuts them down until the ransom is paid.

Let's take a quick look at some of the most prevalent types of ransomware that exist today:

- **Off-the-shelf ransomware.** Some ransomware exists as off-the-shelf software that cyber criminals can purchase from darknet marketplaces and install on their own nefarious servers. The hacking and encryption of data and systems are managed directly by the software running on the servers of the cyber criminal. Examples of off-the-shelf ransomware include Stampado and Cerber.
- **Ransomware-as-a-Service.** CryptoLocker is perhaps the most well-known RaaS model. Since its servers were taken down, CTB-Locker emerged as the most common RaaS attack method. Another RaaS that is rapidly growing is Tox, a kit that cyber criminals can download. The result produces a dedicated executable file that can be installed or distributed by the cyber criminal, with 20% of gross ransoms being paid to Tox in bitcoin.
- **Ransomware affiliate programs.** The RaaS model uses affiliate hackers with a proven track record to spread the malware.
- **Attacks on IoT devices.** Ransomware infiltrates IoT devices that control systems critical to a business. It shuts down those systems until a ransom is paid to unlock them.

Interestingly, in addition to polymorphic code, ransomware often uses metamorphic code to change its digital identity while operating the same way. This rapid growth and constant evolution make it even more difficult for organizations that rely on traditional signature-based antivirus solutions to keep pace. By the time one strain has been identified and blacklisted, cyber criminals have already moved to a new variation. The Ryuk and Sodinokibi ransomware families, for example, both contributed to an increase in the ransom amounts demanded by attackers in Q1 of 2020.[4]

Ransomware Targets

Virtually every operating system is targeted by ransomware today. Attacks also extend to the cloud and mobile devices. The cloud had been left largely untouched by ransomware, so it's a new market opportunity for hackers.[5]

Cyber criminals also target nearly every industry. In 2020 alone, CISA issued alerts about ransomware targeting pipeline operations, healthcare, the public sector, K-12 schools, and more.

Another recent strategy of ransomware hacktivists is to target and compromise vulnerable business servers. "The DearCry ransomware targeting the newly discovered vulnerabilities in Microsoft Exchange in early 2021 is a good example of this tactic, as well as demonstrating the agility of cyber criminals."[6] By targeting servers, hackers can identify and target hosts, multiplying the number of potential infected servers, and devices on a network. This compresses the attack time frame, making the attack more viral than those that start with an end-user. This evolution could translate into victims paying more for decryption keys and an elongation of the time to recover the encrypted data.

These industry alerts were issued in 2020:[7]

- 12/10/2020: AA20-345A (K-12)
- 10/28/2020: AA20-302A (Healthcare)
- 10/28/2020: AA20-302A (Public sector)
- 12/18/2020: AA20-049A (Pipeline operations)

Conclusion

The financial impact of ransomware is much larger than just the ransom being paid to cyber criminals. Downtime translates into thousands, hundreds of thousands, or even millions of dollars in lost revenue and productivity. Organizations across multiple industry sectors can attest to these implications.

Piecemeal approaches to security are not sufficient to thwart ransomware attacks. Integrated models enabling layered security using next-generation firewalls (NGFW), modern endpoint security, and more are required. These security controls must also use proactive threat intelligence when mounting a defense against cyberattacks.

[1] Jonathan Holmes, et al., "Cyber Summit 2020: Trends and Predictions in Ransomware," Federal Bureau of Investigation, 2020.

[2] "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Fortinet, February 2021.

[3] "Most common delivery methods and cybersecurity vulnerabilities causing ransomware infections according to MSPs worldwide as of 2020," Statista, February 16, 2021.

[4] David Bisson, "Increase in Ransomware Demand Amounts Driven by Ryuk, Sodinokibi," Tripwire, May 4, 2020.

[5] Corey Nachreiner, "Why Ransomware Will Soon Target the Cloud," Dark Reading, February 11, 2020.

[6] "New DearCry Ransomware Targets Exchange Server Vulnerabilities," FortiGuard Labs, March 12, 2021.

[7] "Ransomware Alerts and Tips," Cybersecurity and Infrastructure Security Agency, accessed April 28, 2021.

FORTINET

www.fortinet.com

May 2, 2021 2:25 AM

D:\Fortinet\2021 Rebranded templates\White paper\April\Refresh\Ransomware\wp-FA-ransomware-the-exploding-cyberthreat-4292021\wp-FA-ransomware-the-exploding-cyberthreat-4292021

679688-A-0-EN