NEW RANSOMWARE TRENDS IN 2022

Over the past decade, ransomware has become a focal cyberattack method. What started as the encrypting of an individual's files has evolved into threats that are more dangerous and sophisticated. Exploits that were unknown a few short years ago such as country-level extortion and cross-platform execution are now commonplace.

In 2022, there are five new ransomware trends you need to know about as it is highly likely they will be threats for years to come. In this paper, you will learn how these new ransomware threats work and what you need to do to protect your organization against them.

Trend #1 Cross-platform execution

Cross-platform ransomware has become increasingly popular with cybercriminals to penetrate complex environments with multiple operating systems. The goal with this exploit is to cause maximum disruption by encrypting multiple networks and systems.

Ransomware groups have accomplished this by using cross-platform programming languages such as Rust and Golang. This has allowed their malware to spread to devices running operating systems other than Windows, such as iOS, Android, and Linux.

For example, a new cross-platform ransomware dubbed Luna can encrypt files on Windows, Linux, and ESXi. However, the developers are allowing only Russian-speaking affiliates to use it, signaling possible geopolitical motivations. Such targeting of an enemy organization has been seen with Russian cybercriminals attacking the Ukrainian government, which the world has experienced[1] since the start of the Russian-Ukraine war.

[1] Eduard Kovacs, "New Cross-Platform 'Luna' Ransomware Only Offered to Russian Affiliates," Security Week, July 22, 2022.

Luna underlines the newest trend for cross-platform ransomware. Other notable examples include the BlackCat and Hive groups, targeting Linux systems. The Linux sample of BlackCat is similar to the Windows exploit, and it has more capabilities as it can shut down the machine and delete ESXi VMs.

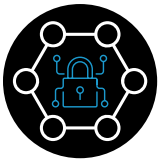
To combat the introduction of cross-platform ransomware, CISOs and IT leaders are recommended to do the following: keep software updated on all devices, focus your defense strategy on detecting lateral movements, set up offline backups, and pay special attention to outgoing traffic to detect suspicious connections.

Trend #2 The rise of Ransomware-as-a-Service

The emergence of the Ransomware-as-a-Service (RaaS) model illustrates a shocking trend: RaaS operators handle the technical backbone of the ransomware operation, while their affiliates focus solely on attack and exploitation methods. This eliminates the affiliates from having to tackle research, development, and ransom negotiations—allowing them to focus solely on exploitation techniques.

The availability of cheap and ready-to-use attack tools has vastly lowered the barrier to entry for cybercriminals to launch devastating attacks. As a result, your organization needs to prepare against a new wave of ransomware attacks.

Defending against RaaS is the same as preventing any other ransomware attack. Because it is so easy to get started, RaaS represents a dangerous new trend. Let's review cyber security best practices to protect your organization from these threats:



Implement critical security protocols that prevent these attacks from having a wider impact on your network. If hackers can't access highly privileged accounts, then they can't spread ransomware widely, move laterally, exfiltrate data, or impact security settings.

Perform regular and frequent backups. If a backup is only performed once a week, then a ransomware attack could devastate an entire week's worth of work.

Implement reliable endpoint protection that can work on zero days and automatically quarantine infected machines.

Maintain a consistent patch program to protect from known and unknown vulnerabilities. Regularly review legacy configurations and misconfigurations, and fix poor credential hygiene practices.

Trend #3

Ransomware targeting cloud deployments

As organizations continue to move workloads into the cloud, ransomware actors have adapted their tactics and procedures to be more cloud native by compromising data stored in cloud services.

As a result, now is a good time for organizations to defend against this threat.

According to a survey [2] of 750 cloud decision makers, at least 50 percent of organizations plan to store data on public cloud services in the future.

BUSINESSES ARE MOVING SENSITIVE DATA INTO THE PUBLIC CLOUD

Type of data that will move to public clouds (% of survey respondents)

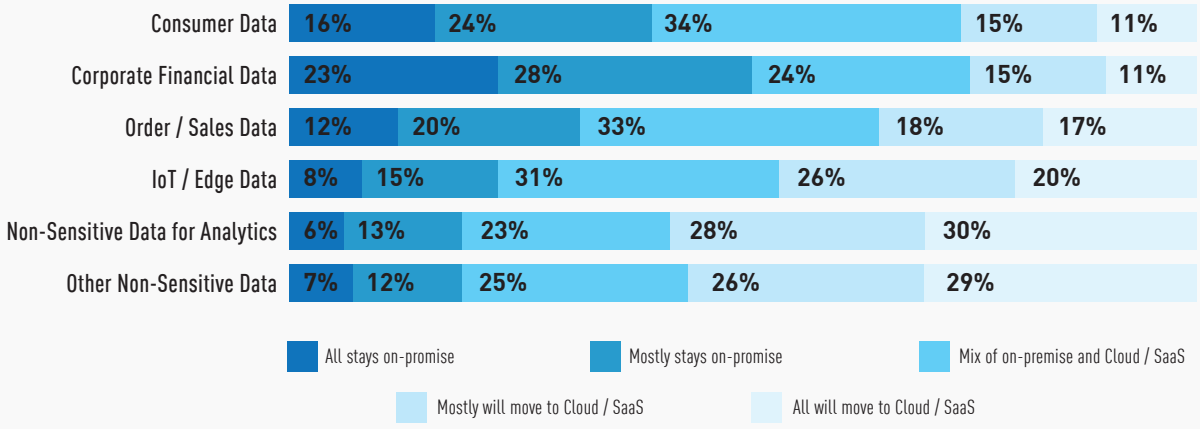


Figure 1: Public cloud transformation table from: "Ransomcloud: How and why ransomware is targeting the cloud." Tech Monitor, Claudia Glover, October 11, 2021, https://techmonitor.ai/technology/cybersecurity/ransomcloud.

[2] Claudia Glover, "Ransomcloud: How and why ransomware is targeting the cloud," Tech Monitor, October 11, 2021.

There are three main ways in which ransomware infiltrates the cloud.

First, it can start on a victim's local device before spreading to the cloud when both the cloud service and the victim's data sync. To defend against this threat, endpoint security and regular patching are recommended.

Second, criminals can get direct access to an organization's cloud servers via phishing, and then they encrypt or extract the data. The most effective defense against this phishing threat requires employee awareness training.

Third and finally, attackers can directly target a cloud service provider to get access to its customers' data. However, this is extremely rare and there aren't many known cases of this occurrence. Here is why: your cloud environment is not simply a copy of your onsite data center and IT systems. The cloud is driven by APIs, and a properly-architected cloud environment ensures that there are multiple copies of your data. This negates the threat actor's main ability to use ransomware. If an attacker encrypts your data, you can simply use the latest version of the data prior to getting locked out.

Public clouds offer reliable and scalable storage services that on-premises data centers would find extremely difficult to keep up with. However, as cloud adoption becomes more prevalent, cybercriminals will find new ways to exploit this attack vector—and organizations will need to adapt.

Trend #4 Country-level extortion

One disturbing trend from the past year has been the emergence of country-level extortion attacks. In a traditional ransomware attack, the attacker demands payment for the decryption key. This has evolved into digital extortion, which threatens to expose the data if the ransom is not paid. Threat actors are now extorting countries, threatening the very fabric of society.

On May 12, Costa Rica's president declared a state of national emergency. Days later, the president announced that the country is at war against a cybercrime group dubbed Conti.

What happened? The Conti group breached and encrypted over 27 of Costa Rica's governmental agencies. When the government refused to pay the ransom, the group encouraged the citizens of Costa Rica to protest and overturn their government.

While this likely started as a normal ransomware attack, it quickly turned into a new type of threat with far-reaching financial and geopolitical consequences.

Furthermore, Conti publicly vowed to protect the Kremlin and threatened to retaliate with all its resources against any enemy that threatens Russian organizations. They claimed that they would cause serious damage to the critical infrastructures of any enemy entity. After Conti's declaration, a leak of the groups' internal communications was dumped on the internet. Check Point Research (CPR)[3] analyzed the Conti leaks and discovered that the intricate layers and hierarchy within the group were similar to those of a corporation. Following this, Conti increased the rate of its attacks, increasing from 10 victims in January to nearly 80 in April.

"Country extortion" is clearly here to stay. If you're responsible for defending the public sector, then you'll need to put defense strategies in place that will improve your local, state, and federal agencies' security postures. See below for several recommendations:

User Awareness Training

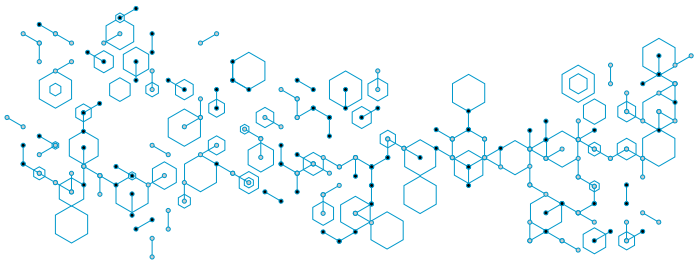
According to reports, 91%[4] of all cyber attacks begin with a phishing email to an unsuspecting victim. Incorporate phishing simulation into your employee training programs to ensure that users can identify and avoid these cyber attacks. Even your most tech-savvy people can fall prey to a well-architected phishing exploit. Social engineering scams have become so sophisticated that criminals are using artificial intelligence to fake the voice of executives and demand payment from subordinates. Phishing-detection systems can help pick up subtle cues and block e-mail threats.

Continuously Monitor and Diagnose the Environment

To shed light on malicious activity, you must have full visibility and understanding over your network. For example, the U.S. Department of Homeland Security (DHS) launched the Continuous Diagnostics and Monitoring (CDM), allowing agencies to better monitor their IT systems in real-time and address vulnerabilities instantly. The program lets you know what's occurring in a network on a continuous basis—not just at audit time. A similar program can provide your IT staff with real-time configuration monitoring against a library of security best practice diagnostics to ensure security and compliance.

3 "Leaks of Conti Ransomware Group," Check Point Research, March 10, 2022.

4 Stu Sjouwerman, "91% of cyberattacks begin with spear phishing email," KnoeBe4, November 29, 2021.



Transition to Cloud-Based Technology

On-site servers are not only expensive but are also vulnerable for hackers to exploit. Nonetheless, hundreds of government agencies continue to rely on them to store sensitive data. Making the journey to cloud-based government management software will allow agencies to securely store data off-site with certified cloud providers. Automatic backups also enable business continuity and allow agencies to maximize operational uptime.

Compliance and Zero Trust

Governments must focus on solutions that comply with data protection frameworks such as GDPR, CCPA, HIPAA, CJIS, NIST 800-171 and then implement several key strategies for data protection using the Zero Trust philosophy. With a remote workforce, combined with the increase in devices and endpoints, data has become extremely vulnerable—hence the shift towards Zero Trust. This involves privacy and authentication (control over who has access to your organization's assets while verifying their identity) as well as safety (allowing employees to access critical data when necessary).

Public sector agencies that lack sufficient support or IT resources should look at collaborating with an MSP. Sometimes, an MSP can be faster than building a security team from scratch while improving an organization's security posture. Doing so can also reduce costs related to training and hiring.

Trend #5 IoT ransomware attacks that can move laterally

IoT ransomware infections may set the stage for future cyber attacks. This potential attack vector is based on the rapid growth of IoT devices.

One organization developed Ransomware for IoT[5], or R4IoT, to prove that ransomware can exploit an IoT device and move laterally in an IT network. Its goal? To exploit vulnerable IoT devices such as IP cameras, and then deploy ransomware that will hold critical processes hostage.

5 Ravie Lakshmanan, "Researchers Demonstrate Ransomware for IoT Devices That Targets IT and OT Networks," The Hacker News, June 2, 2022.

If R4IoT proves that IoT devices can be compromised, then attackers can add an additional layer of extortion to a traditional ransomware attack by holding IoT, IT, and OT assets hostage. Furthermore, attackers could not only drop ransomware but also launch additional payloads such as DoS attacks against OT assets.

To protect your IoT devices, organizations should patch vulnerabilities in their devices, implement strong password hygiene, enforce network segmentation, and monitor connections and network traffic.

Conclusion

Ransomware groups have come a long way from being disorganized criminals to full-fledged businesses operating like a corporation. As a result, cyberattacks have evolved and become more sophisticated, exposing companies to more sophisticated and dangerous threats.

To protect against these advanced threats, you need to start preparing now. Because once your network is compromised, it's already too late.

For more information on how the underground ransomware economy works, visit Check Point Research's recent coverage.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com