Cyber Security Trends Forecast - 2022

January 2022

Cyberint

TABLE OF CONTENTS

INTRODUCTION

As we go into 2022, looking back at the plentiful year of 2021, regards to security, we at Cyberint Research Team will try and shed some light on the upcoming year: What we consider the key security risks and threats, and what we feel will change in the coming year. We will focus on the actions required to be as vigilant and protected as possible.

Although we foresee that, for example, Deep-Fake news will rise and mobile applications will also be in danger, thanks to the increased use of mobile wallets, we chose to focus on the lowest common denominator relevant to most companies, as well as our customers.

This report predicts that in 2022 most of these will be intertwined, since, for example, a threat actor could combine the following tools and techniques to further expand and broaden their business.

CLOUD SERVICES

In the last few years, cloud services have become mainstream. The pandemic-style of work made an impact, and pushed more and more companies to adapt and migrate to the cloud to facilitate the continuation of work. This era of Work from Home (WFH) has become as standard as making a cup of coffee.

Our prediction is that more and more companies will continue to migrate to the cloud, as more "Somethings"-As-A-Service continue to appear. Another prediction is that after companies adopt cloud services, the move to multi-cloud service providers, for various reasons, such as pricing, availability, and more, will also rise.

Consequently, more cloud-native attacks will start to occur. Attacks will vary based on the threat actor's ability to orchestrate an attack on the cloud, from the mid-2021 simple case of the Cosmolog Kozmetic [1] data leak, which concluded in a misconfigured and exposed AWS S3 bucket, exposing customer purchases to more fairly "sophisticated" attacks, such as the TimeHop database incident [2], or CapitalOne XSRF case [3].

Born-in-the-cloud companies will find it easier to set up their cloud security posture, while we believe the migrating companies, will have some trouble adjusting to the new style of work and terminology.

Most of the cloud breaches we have already seen usually come down to misconfigurations, overly permissive permissions, or unprotected public-facing servers. They all come down to the lack of visibility one has on the cloud, when a single click can instantiate hundreds of machines, sometimes without the true ability to tell if they are publicly exposed or well-protected.

"Shift-left" protection over Infrastructure-As-A-Code (IAC) will continue to take place in the cloud infrastructure and security, as it ensures that tighter security practices are implemented earlier in the process, and not just as a last step in the lifecycle.

Companies migrating to the cloud should take into consideration the shared responsibility model, and understand that migrating to the cloud, doesn't always mean that the cloud will handle everything,

let alone when it comes to security. Companies should understand the different functions they need from cloud vendors, identify the critical points, such as sensitive data, who can access what resources, what can they do with that resource, and knowing what actions that user took, given any incident.

RANSOMWARE

Ransomware remains a growing and increasingly problematic threat to organizations across all industries. Posing a significant and increasing threat throughout 2021, "Big game hunter" ransomware campaigns, orchestrated by highly sophisticated organized cybercriminal groups, continue to compromise and extort high-value ransoms from victim organizations across all industries. While statistics related to ransomware activity over the past year differ, all are consistent in identifying a week-on-week increase in attacks.

Cyberint findings of a **rise of 84%** in ransomware cases in H2 of 2021 compared to H1 of 2021, shows the massive growth of the ransomware industry worldwide.

TACTICS TECHNIQUES AND PROCEDURES

Typically, major ransomware groups utilize "steal, encrypt and leak" tactics, pressuring their victims into paying high-value ransoms to avoid exposure. These groups continue to evolve their tactics, techniques, and procedures (TTP), with new developments and recruitment, undoubtedly fueled by the enormous financial gains being made. Although the TTPs often evolve, the foundation remains the same:

1. Victim reconnaissance
2. Initial infection
3. Post intrusion
4. Encryption phase
5. Ransom note

BACK TO THE ROOTS

Although most commonly, these threat groups often use the double-extortion technique, evidence suggests that ransomware groups are following an "old-new" trend of focusing on compromising data without encryption and demanding ransomware to not leak the sensitive data. This trend puts the threat groups into a position where their franchise can only focus on implementing fewer elements in their campaigns and focusing only on infiltrating the victim's network and exfiltrating the data while the encryption phase left out. Cyberint has witnessed cases where backup services have successfully restored the encrypted data, but the victims still were paid the ransom to prevent the data leakage. This situation led some threat groups to realize that the encryption phase may not be always necessary for a successful campaign.

ORGANIZATIONS VS. LAW ENFORCEMENT AUTHORITIES

As ransomware has become more popular, spreading over regions and sectors, a new challenge arose as a result of the conflict between law enforcement authorities and organizations that were successfully attacked by ransomware. While the former urge the victims to refuse to cooperate or negotiate with the ransomware groups, the latter's interests are to mitigate and restore the stolen data and get the organization back on track as soon as possible.

While we observed cases where threat actors restored only around 60% of the stolen data once the ransom was paid in 2020, ironically, they improved their "reliability" while restoring a much higher percentage - around 90% - to the victims.

EVERYONE HAS A PLACE

Off-the-shelf threats and Ransomware-as-a-Service (RaaS) offerings remain available via underground forums and marketplaces. While many of the known threats may be considered old, many variants have been spawned from leaked source code. RaaS offerings somewhat remove the entry barrier and allow low-sophistication threat actors to purchase tools that can be used to launch attacks or, in some cases, freely distribute a ransomware threat to victims in return for commission whenever a ransom is paid.

Although individuals may still be targeted in indiscriminate ransomware campaigns, they are unlikely to offer good ransom returns and therefore, many low-sophistication threat actors appear to be targeting small and medium-sized enterprises (SME), making the campaigns much more profitable with reasonably low risk given the fact that medium and small enterprises might not get the same attention in the media and from law enforcement.

As expected with low-sophistication threat actors, techniques such as spear-phishing campaigns are typically used to deliver their ransomware threats via weaponized email attachments, potentially selecting victims from harvested email address lists rather than conducting reconnaissance on, and targeting, a specific organization.

RANSOMWARE AS A SERVICE COMPETITION

As mentioned, the ransomware industry enjoys massive growth - Alongside it, the sector of Ransomware-as-a-Service (RaaS) claims newcomers that offer better terms to members that will join the service (Figure 1) compare to other RaaS. We are likely to witness more services that get into the game offering better fees, minimal distribution effort, better anonymity, "noob-friendly" and more.

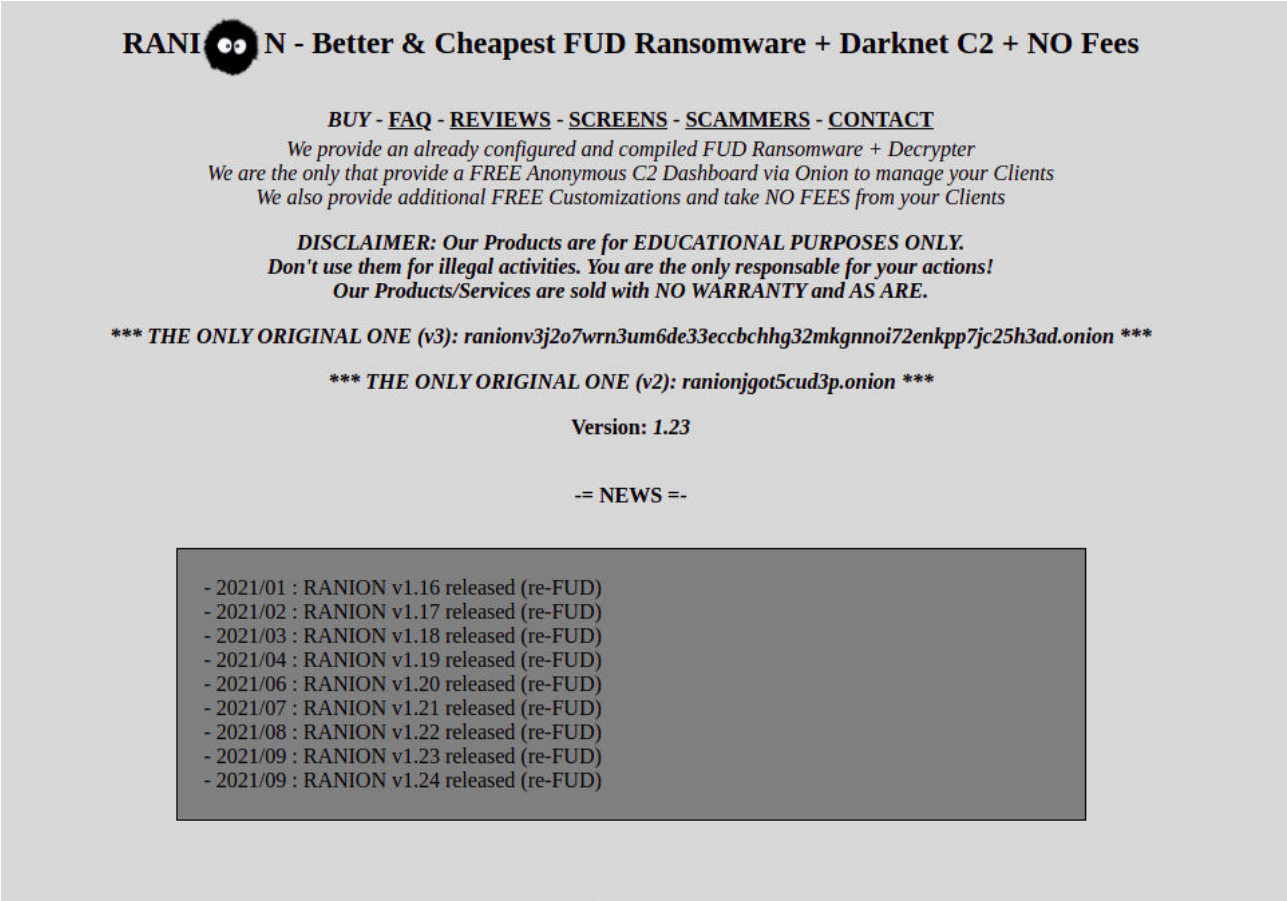

Figure 1: New Random-As-A-Service example, one of many that have arrived this year

We already witnessed two new fairly successful RaaS families that emerged in 2021:

AvosLocker emerged around June 2021 and has already made significant progress on establishing its services as one of the more successful new families relative to how long they've been operating.

Khonsari ransomware has claimed the place of the first ever ransomware group to utilize the Log4Shell vulnerability in their campaigns.

In following both AvosLocker and Khonsari, we have witnessed in underground forums and chatters that they are looking to expand their operations and looking to recruit new members.

INFO STEALERS

Since May 2021, we have observed a rise in Stealer campaigns. Redline, Raccoon and Oski were the most common, with a 100-300% spike.

Info Stealers development became popular within Russian underground forums and Telegram channels (Figure 2) that wish to sell this type of content. Additionally, given that it has become a sweet spot between high income and low priority for law enforcement, we will see threat actors creating a long-term product, releasing weekly updates.

Figure 2: Redline Telegram official channel.

As for classic stealers, most will try to obtain sensitive information like usernames, passwords and cryptocurrency wallets. Given the growing numbers of users and investors around the world, both in cryptocurrency and NFTs, 2022 holds massive improvements in the cryptowallets exfiltration mechanisms.

The most common stealer families (Figure 3 below) are Redline and Raccoon. As the stealer industry grows, we are starting to observe new campaigns combined by several stealers using the “best qualities”. For example, campaigns combining AgentTesla's delivery methods, Raccoon's and Vidar's data exfiltration and Redline's backdoor deployment. Although campaigns of this scale are not that common, we are seeing a rise in these cases, suggesting that threat actors are finding creative new ways to combine several stealers in the process.

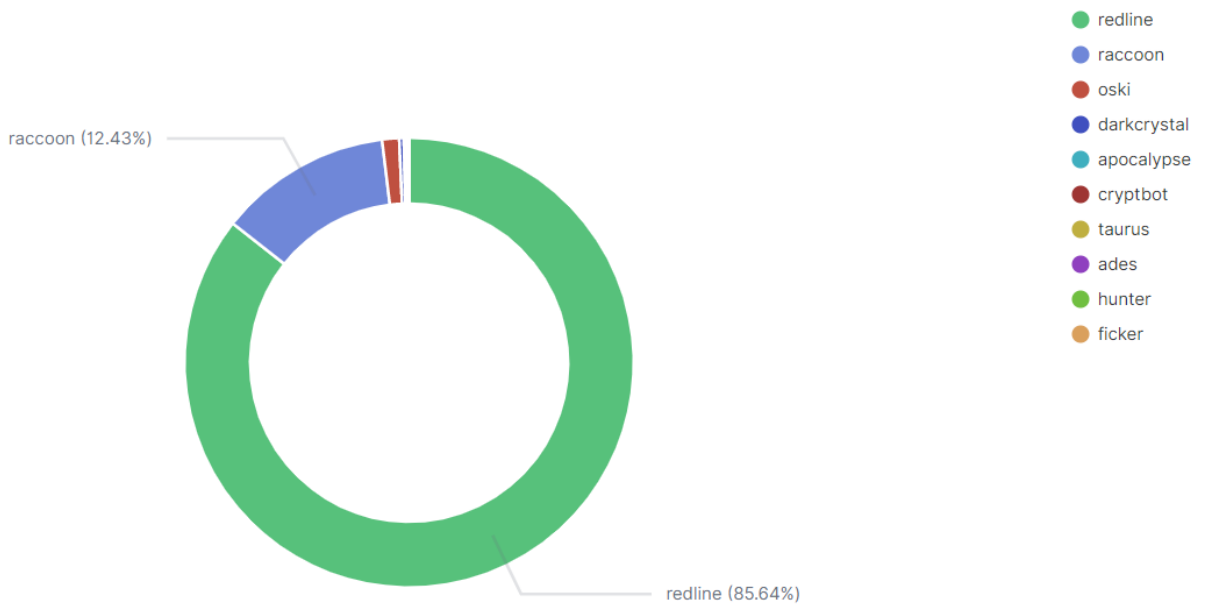

Figure 3: Top 10 Info Stealers

VULNERABILITY EXPLOITATION

Vulnerability exploits are the means by which a vulnerability can be used for malicious activity by different threat actors. Some are published by the vendors themselves, some are published by the community as POCs, while some go undetected by the community, but are used by threat actors as another tool in their arsenal.

Threat actors used these for years, and our assumption is that the older vulnerabilities, (disclosed in past years) will not lose their traction among threat actors, and will be combined with the newly not-yet discovered vulnerablities.

After a pretty decent year in application vulnerability exploits, setting a record number of published zero-days [https://www.technologyreview.com/2021/09/23/1036140/2021-record-zero-day-hacks-reasons], we can only predict that the numbers will break records again in 2022.

As more vulnerabilities are expected to appear, enterprise and service companies will be on high alert for a potential patch.

When talking about application vulnerability, we must mention the recent Log4j cases that closed 2021, which we believe will pave the way to more vulnerabilities in highly used libraries, packages, and 3rd party applications, with a dramatic impact on the industry.

As the result of a security breach could be catastrophic, it will be in the hands of DevOps engineers, Security teams, and basically, all tech-related company employees, to be vigilant, and alert to such cases as they occur.

Although version control is something that is not trivial to follow as soon as a patch is released for most businesses, we highly recommend setting use cases in which version control is above all other operations within the organization infrastructure if cases such as Log4Shell emerge in 2022.

SUPPLY CHAIN ATTACK

We've seen a rise in Supply-Chain attacks over the past year. Across all threat sectors, each attack is designed for maximum impact, whether it's ransomware seeking as high a payment as possible, or massive infection of info-stealers.

When talking about maximum impact, consider supply-chain attacks, where impacting a single link of the chain, can cause significant damage along the entire supply chain.

Looking back on recent events related to supply-chain attacks, two major incidents caught the industry's attention.

First, the SolarWinds case, which involved DLL infection in the infrastructure, that caused all vendors using SolarWinds product to become infected as well, leading to a wave of strategic infections.

Second, was the Kaseya incident, a managed service provider (MSP), where the company suffered a ransomware attack by the REvil (aka Sodinokibi) ransomware gang, that led to ransomware propagation to Kaseya's customers.

Supply chain attacks can also result in real-world problems, such as the Colonial Pipeline incident, which caused a fuel shortage due to temporary shutting down of factories; or the JBS Foods incident, which shut down some operations in Australia, Canada, and the US, which led to shortages of meat and increased prices for consumers.

We believe that since the impact is huge, compared to personal machine malware infection, or even a single company breach, threat actors will target supply chain attacks, which are here to stay. More cases will emerge in 2022, causing damage, not only internally to the compromised company, but to its customer's customers.

Companies will have to adapt and make sure their vendors are also secure.

WFH – SECURITY CHALLENGE

As a result of the COVID-19 pandemic, a new workflow era has emerged. In our new reality, an employee can continue to work from a coffee shop, hotel room, or home office.

The Work-from-home attitude, courtesy of COVID-19, is here to stay for the foreseeable future - that's a fact. If 2020 paved the way for a more applicable work-from-home approach, 2021 set the tone further, with IT switching its focus to enable working from home, and for 2022 we can only assume that this work method will continue.

However, with the ease of working in your pajamas, comes great responsibility in terms of security.

Threat actors understand the tendency of most people to mix social and professional platforms when they work from home regularly. This makes the personal gain of a successful campaign much more profitable.

Work-from-home causes security to loosen up, borders to be breached, and many employees will continue to use their own home equipment and their home Wi-Fi, rather than company devices protected by IT or security teams.

Although most campaigns look for more obvious valuables such as cryptocurrency wallets and private credentials, the risk of a threat actor gaining business email information or VPN client credentials becomes more real and its severity in the ransomware era we live in might be critical.

As many employees work from home or adapt to increased online habits, they should be reminded to be suspicious of any unsolicited or unusual communication, especially those containing attachments or links, as well as to be mindful of any websites they visit using corporate assets. Furthermore, a repetitive reminder of the importance of the matter, and the consistent use of VPNs for work purposes, might help keep employees alert and aware of the threats of working from home.

REFERENCES

[1] HTTPS://SECURITYAFFAIRS.CO/WORDPRESS/119067/DATA-BREACH/COSMOLOG-KOZMETIK-DATA-BREACH.HTML
[2] HTTPS://WWW.TIMEHOP.COM/SECURITY
[3] HTTPS://WWW.CAPITALONE.COM/DIGITAL/FACTS2019/
[4] HTTPS://WWW.TECHNOLOGYREVIEW.COM/2021/09/23/1036140/2021-RECORD-ZERO-DAY-HACKS-REASONS
[5] HTTPS://CYBERINT.COM/BLOG/RESEARCH/REVIL-KASEYA-INCIDENT-UPDATE/
[6] HTTPS://CYBERINT.COM/BLOG/RESEARCH/SOLARWINDS-SUPPLY-CHAIN-ATTACK/

CONTACT US

www.cyberint.com | sales@cyberint.com | blog.cyberint.com

USA

Tel: +1-646-568-7813
214 W 29th St, 2nd Floor New York, NY 10001

ISRAEL

Tel: +972-3-7286-777
17 Ha-Mefalsim St 4951447 Petah Tikva

UNITED KINGDOM

Tel: +44-203-514-1515
Fox Court 14 Grays Inn Rd, Holborn, WC1X 8HN, Suite 2068 London

SINGAPORE

Tel: +65-3163-5760
135 Cecil St. #10-01 MYP PLAZA 069536

LATAM

Tel: +507-395-1553
Panama City