Threat Landscape by the Numbers 2021 and Beyond

January 26, 2022

Ed Cabrera, Chief Cybersecurity Officer
Lexi Cormier, South Florida Account Manager
lexi_cormier@trendmicro.com, 407-435-8118
Global Threat Landscape

The Trend Micro™ Smart Protection Network™ is a global network of threat intelligence sensors with continually updated email, web, and file reputation databases in the cloud. This up-to-the-second threat intelligence allows us to identify and block threats in real time.

The Trend Micro reputation services check widely-used threat vectors to block spam/phishing, compromised websites, malicious files, compromised devices, and malicious mobile apps. They are:

- Email Reputation Service (ERS)
- Web Reputation Service (WRS)
- File Reputation Service (FRS)
- IoT Reputation Service (IOTRS)

*These figures are approximate to show the SPN scale*
Total Threats – Blocked (Annual)

The threats blocked have shown an upward trend since 2018. And there is a significant increase from 2019 to 2020, especially in WRS. While the total in 2020 was 66.5 billion, as of November 2021, 2021’s data has already reached 85.6 billion.
Extended exposure leads to active compromise

- Approximately ~770 vulnerabilities, with ~66 zero-days, have been found in Y2021.
- Increased risk due to shorter time these were weaponized.
- Customers are still challenged to address the “patch gap”, and are lagging behind.

Vision One Workbench Alert for “Possible Web Service Abuse”, for a Microsoft Exchange Server. Managed XDR declared multiple incidents on this single environment on this host, due to lapses in patching a Microsoft Exchange vulnerability (CVE-2021-26855), what was disclosed on Q3 2021. Last incident happened 2021/11/03.
Covid-19 (related threats)
Email, URL, Malware and by Country data
Covid-19 by Month (Email, URL, and File)

Most of the threats riding on Covid-19 topics are through emails. And there was a significant decrease from May to June. But again, we saw a slight increase from July and August. This November, we still see the active trend of this threat, although the detection fell below 500,000.
Most of the threats riding on Covid-19 topics are through emails. And there is a significant decrease from May to June. But again, we saw a slight increase from July to August. In November, for all three protection layers, we saw a decrease.
Email & Web Threats
Phishing, Spam Attachments and BEC
Total Threats – Blocked (Annual)
PDF has regained top position from October to November with a spike of 891.7%, though we did not observe any significant spam outbreak. Due to this spike, the total counts also showed a massive 221.0% increase.
In November, the overall BEC attempts showed a 38.5% increase, and yet keeping the plateau, the spike level from August is still intact. On the other hand, the CEO fraud also showed a 3.4% increase from October to November.
From October to November, the manufacturing industry holds the top spot. The healthcare vertical decreased from 22,907 to 19,906, which dropped one place, falling to the fourth place, surpassed by the government and education sectors.
The government vertical took the top spot for November, taking it from the technology sector, which fell to the seventh. The healthcare industry also dropped to the fourth position, decreasing from 141 to 102.
EMOTET, RYUK, and TRICKBOT are the three malware families with the most active campaigns. Return of Emotet: One of the most dangerous and infamous botnets in history, is back. Since Emotet’s November return, we found the malware’s activity to be at least 50% of the level seen in January 2021, shortly before its initial takedown. This rising trend continued throughout December with several end-of-year campaigns, and is expected to continue in 2022, at least until the next takedown attempt.
EMOTET shows an increase in enterprise and SMB segments. While the collaboration of these three families is still significant, the return of EMOTET could be more from its independent move. And the target is still dominantly the enterprise sector.
Ransomware Threats - Excluding WCRY

The chart shows the monthly trends without WCRY. In November, it indicates a slight increase in detections. Excluding its influence, we can see the rise of the other ransomware families during the fourth quarter of 2020 and the third of 2021.
Ransomware Families – Industries

In November, the healthcare industry increased from 1,189 to 1,894, making it the top sector. And the government sector dropped to the second position which also increased from 1,409 to 1,657.
Ransomware remains a top threat

- Publicly accessible services and applications has fueled ransomware attacks directly on servers.
- The Ransomware threat has been observed as one of the main goals of such compromises, across all regions.

- Attempts for cryptocurrency mining has also been seen as an end-goal.
- At some incidents, the end-goal of the intrusion may not be immediately obvious.
... and more Ransomware ...

- In Y2021, attacking the "supply chain" came to the spotlight – again.
- Threat actors may attack the supplier, rather than single compromises, which may yield more gains.
- General shift: Espionage with the Solar compromise (Sunburst, Solorigate, Nobellium) vs. Ransomware with Kaseya VSA Supply Chain Attack (REvil/Sodinokibi)
Our research teams have discovered two new ransomware families in November, which is lower, unlike the previous months, while we saw ten families in January. Still, attackers constantly create new ones, working for the "next" high-profile ransomware families, even the RaaS business model.
### Double Extortion Ransomware Families

<table>
<thead>
<tr>
<th>Aug-21</th>
<th>Sep-21</th>
<th>Oct-21</th>
<th>Nov-21</th>
</tr>
</thead>
<tbody>
<tr>
<td>AVOS/AVOSLOCKER</td>
<td>LOCKFILE</td>
<td>BLACKBYTE</td>
<td></td>
</tr>
<tr>
<td>HIVE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>As of Mar 2021</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AGELOCKER</td>
<td>Everest</td>
<td>RAGNAR</td>
<td></td>
</tr>
<tr>
<td>AKO/MedusaLocker</td>
<td>EXX/DEFRAY777</td>
<td>Ragnarok</td>
<td>GRIEF</td>
</tr>
<tr>
<td>ALUMNILOCKER</td>
<td>HADES</td>
<td>RansomExx</td>
<td>(DOPPELPAYMER renamed)</td>
</tr>
<tr>
<td>AVADDON</td>
<td>LOCKBIT</td>
<td>Ranzy Locker/ThunderX</td>
<td></td>
</tr>
<tr>
<td>BABUK Locker</td>
<td>MAZE</td>
<td>RYUK</td>
<td>PAYLOADBIN</td>
</tr>
<tr>
<td>CLOP</td>
<td>MESPINOZA/PYSA</td>
<td>SEKHMET</td>
<td></td>
</tr>
<tr>
<td>CONTI</td>
<td>MountLocker/AstroLocker</td>
<td>SNATCH</td>
<td></td>
</tr>
<tr>
<td>CRYLOCK</td>
<td>NEFILIM</td>
<td>SODINOKIBI/REvil</td>
<td>THUNDERCRYPT/Lorenz</td>
</tr>
<tr>
<td>DarksIDE</td>
<td>NEMTY</td>
<td>SUNCRYPT</td>
<td></td>
</tr>
<tr>
<td>DOPPELPAYMER</td>
<td>NETWALKER</td>
<td>THANOS</td>
<td>Apr-21</td>
</tr>
<tr>
<td>EGREGOR</td>
<td>pay2Key</td>
<td>XINOX</td>
<td>NETWORK/N3tw0rm</td>
</tr>
<tr>
<td>EKANS</td>
<td>PROLOCK</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Cybercriminals didn't just deny access by encrypting their victims’ files; they also started to threaten to expose the files if the target didn't pay the ransom. Moreover, they even conduct DDoS attacks and direct communications with victims or their customers. So, the attack is not only double but even triple, quadruple, or multilevel extortions. In November, our research teams didn’t find any additional family.
Financial Threats

Banking and PoS Malware Types
Banking Malware

These five banking malware families are constantly in use for cybercriminal activities. Among them, RAMNIT has dominated the top position ever since as one of the most well-used malware families to target bank users. In November, the total number showed a 16.8% increase. It is also notable that EMOTET has kept the higher ranking in the past four months.
Banking Malware – Industries

It’s interesting to see banking malware variants target other verticals. For example, those healthcare, government, and manufacturing organizations are never free from the risk of banking malware attacks. In November, we saw that the government sector took the top.
PoS malware gets information gathered from the credit cards running on the PoS (Point of Sales) system, like how an information stealer benefits from a browser. Their detection counts are insignificant compared to other malware types. Still, in November, we saw a decrease in total, especially ALINAOS.
Cyber Threat Landscape 2022 and beyond
Polarization and misinformation

*AI enabled fake information distribution will move to enterprise /commercial target than individuals*

The polarization and massive distribution of misinformation will be the next digital divide. One of the more popular abuses of AI are deepfakes, which involve the use of AI techniques to craft or manipulate audio and visual content for these to appear authentic. The use of pervasive reliance on complex algorithms /programs will accelerate imbalance and likely bring damage to individuals and amplify societal fractures.
Digital Identity is the new security control and perimeter. Emergence of new technologies and support regulations as Digital Identity will transform given the demand online identity is surging public and private stakeholders demand and rely on it. Issues on data protection, interoperability, compatibility and security will emerge.
Critical infrastructure

extreme digital technologies and adoptions may spawn possible attacks to CI

Advanced countries and economies will continue to rely on massive technological adoptions after covid. This will amplify the attack surface of companies and CI will continue to be an attractive target over its dependence to both domestic and international supply chains.

Challenges of the risk's framework used and adopted by some Cis are build on traditional risk management which is skewed to how interstate digital conflicts, evident in state-affiliated cyberattacks on critical infrastructure.
As the healthcare industry begins to recuperate from a pandemic, securing acquired digital assets becomes a prime security concern. Healthcare will carry the significant burden of data protection as they amassed collective data/intel after the pandemic. The pandemic has allowed healthcare institutions to gather a sizable amount of sensitive patient information not just in hospitals but also in temporary facilities and vaccine centers. The need to secure this deluge of data will be juggled with security efforts for hastening digital transformation.

Digital supply chain will be vulnerable as the online processes, services will be tightly interconnected. While attempts to return to a pre-pandemic lifestyle will be underway, it can be expected that many online services will continue to thrive. Teleconsultation, digital-only banks, electronic shopping, and other online services will remain as lifestyle mainstays. Amplified reliance on these could bring about both known threats (such as socially engineered messages) and enemies which are yet to be seen and when they are compromised the entire supply chain can be exposed.
Scrubbing tactics instead of threat actors themselves will be one of the focal points for securing the cybersecurity landscape.

From a security defender’s point of view, it is often more helpful to know how, instead of why, threat actors are conducting attacks. Such knowledge can help prevent and mitigate current and future schemes. Thankfully, more and more data on these tactics are being documented by both public and private sectors, and we can expect such endeavors to continue.

The need to establish tighter collaboration between organizations and third-party security vendors will be underlined.

As many companies take efforts to adapt to ever-increasing digitalization, such as moving from on-premise to cloud and setting up permanent work from home arrangements, cooperation with security vendors at every step of these processes is an absolute necessity; not merely an option or a last resort.
Ransomware will mutate into an even more menacing threat as it continues to develop a more targeted approach, enhanced accessibility, and additional extortion levels. “Ransomware-drive through“

Ransomware can be made even more readily available. More attacks can also incorporate multilevel extortion techniques that further pressure companies, such as DDoS attacks, directly contacting the target’s customers, hijacking networks, targeting smart cities, and many more.
Investigation into PlugX Uncovers Unique APT Technique

Through the APT One with Endpoint Sensor (IES), we discovered an APT from a company.

By: Gilbert Sison, Abraham Garcia, Ryan Magana
Published: 03/09/2021

Finding and Decoding Multi-Step Obfuscated Malware

Our investigation of an unusual DNS scan by a command-line tool led us to the discovery of a multistep obfuscated malware.

By: Abraham Garcia, Ryan Magana, Samata Lee
Published: 02/03/2021

Chopper ASPX Web Shell Used in Targeted Attack

Authors

Cyber Threats

Tracking Cobalt Strike: A Trend Micro Vision One Investigation

Cobalt Strike is a well-known beacon or post-exploitation tool that has been linked to several ransomware campaigns. This order to fully contain and remove a malware infection.

By: Abraham Garcia, Samata Lee, Ryan Magana, Rudy Tenorio
Published: 01/28/2021

Supply Chain Attacks from a Managed Detection and Response Perspective

In this blog entry, we will take a look at some examples of supply chain attacks that our Managed Detection and Response (MDR) team has encountered in the past couple of months.

By: Ryan Magana, Rudy Tenorio, Ryan Magana, Rudy Tenorio
Published: 12/08/2020

PurpleFox Adds New Backdoor That Uses WebSockets

In September 2021, the Trend Micro Managed IED (MDM) team looked into suspicious activity related to a PurpleFox operator. Our findings led us to investigate an updated PurpleFox malware that included an added vulnerability (CVE-2021-1733) and optimized rootkit capabilities leveraged in their attacks.

By: Joseph Pennar, Jay Vlasky
Published: 09/18/2021

Related Articles

- Build a complete cloud environment
- Understanding Cybersecurity
- Get started with Windows Defender
- Advanced threat protection
- Get Started with the Cloud

Web Resources

- Trend Micro Cloud Security
- Trend Micro Cloud
- Trend Micro Security for Cloud
- Trend Micro Cloud Security
- Trend Micro Cloud Security

Related Articles

- Build a complete cloud environment
- Understanding Cybersecurity
- Get started with Windows Defender
- Advanced threat protection
- Get Started with the Cloud

Web Resources

- Trend Micro Cloud Security
- Trend Micro Cloud
- Trend Micro Security for Cloud
- Trend Micro Cloud Security
- Trend Micro Cloud Security
Thank You

Ed Cabrera, Chief Cybersecurity Officer
Lexi Cormier, South Florida Account Manager
lexi_cormier@trendmicro.com, 407-435-8118