THE ECONOMICS BEHIND CYBERCRIME AND INTELLECTUAL PROPERTY THEFT

How criminals monetize their crimes

Cybercrime pays.

A cyber criminal's 'business plan' is simple: plot an attack, steal/abuse/impact computing-based resources, execute the assault without getting caught, and pass the costs to others. So effective is this plan, in 2021 alone, experts estimate cybercrime cost the world $6 trillion USD[1] By comparison, one source pegs the entire security tools market at around $150 billion by 2025.[2] About 80 percent of all cyber attacks originate from organized-crime gangs including state-sponsored Advanced Persistent Threat (APT) groups.[3]

These lofty figures validate that cybercrime is lucrative, spurring huge increases in attack threats. Check Point Research (CPR) said customers cited a 50 percent jump in overall attacks per week on their corporate networks compared to 2020.[4] The cyber pandemic in 2021 saw the year begin with the massive Sunburst hack against U.S. government agencies and corporations. It was followed by a rash of various ransomware attacks that included supply chain attacks, multiple extortion schemes, and Ransomware as a Service (RaaS) exploits. The year ended with the explosive Log4j code module vulnerability attack that crippled server networks around the globe.

> "Before COVID, we ran our life 50/50 between the physical and cyber worlds, during the pandemic, it became 90/10. Now it is about 80/20. COVID made cyber threats more dangerous."
>
> –Gil Shwed, CEO, Check Point Software

[1] Steve Morgan, Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cyber Crime Magazine, Nov. 13, 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[2] Security Market Size Worth $167.12 Billion By 2025 | CAGR: 10.3%, Grand View Research, June 2019.

[3] Verizon, 2021 Data Breach Investigation Report, page 12.

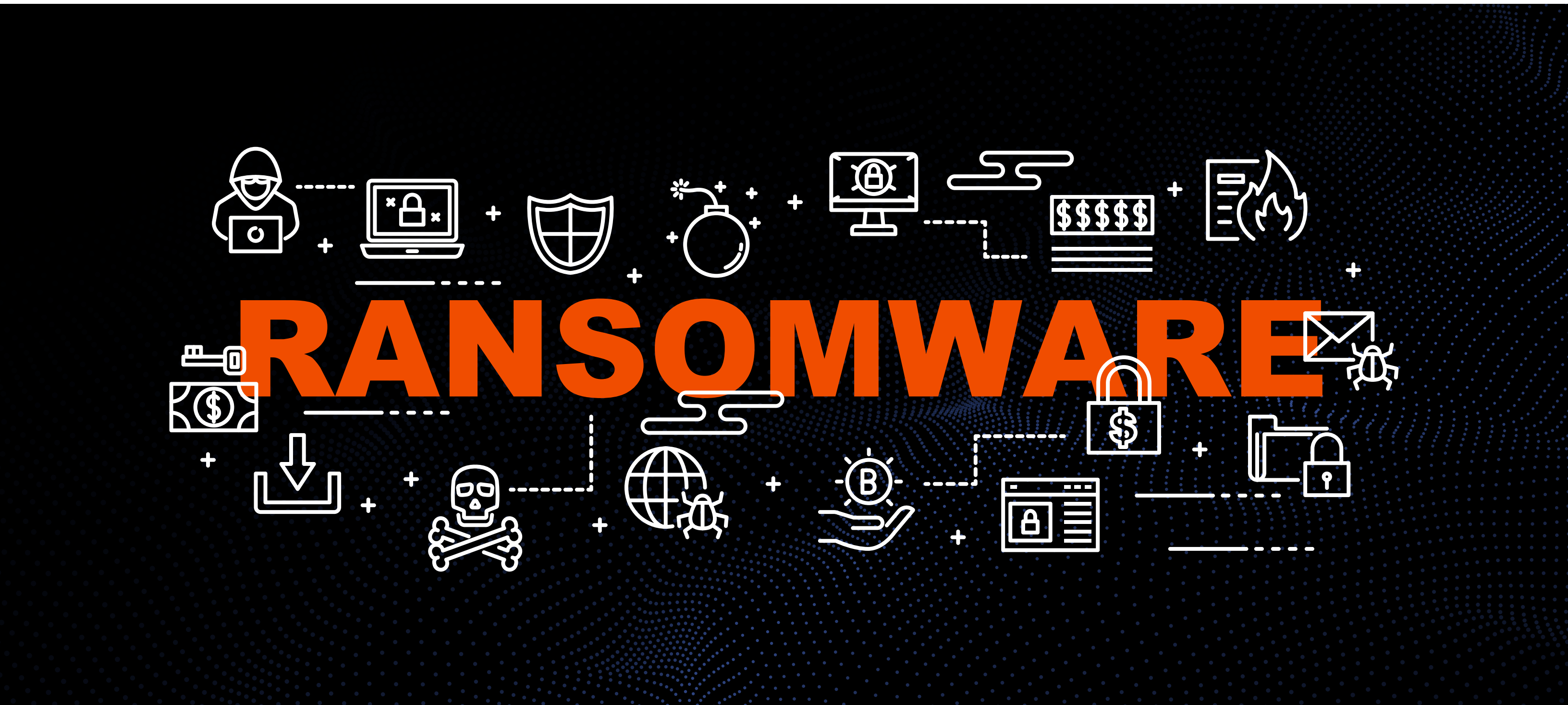
[4] "Cybersecurity: Last year was a record year for attacks, and Log4J made it worse," By Jonathan Greig, ZDNet, January 11, 2022.

Doubling down on ransomware

Though a fraction of some $200 million paid to the REvil ransomware gang (from April 2019 to July 2021), the U.S. Justice Department seized $6 million in ransom payments paid to an alleged REvil operative.[5] REvil is a ransomware-as-a-service that encrypts data in a victim's directory and deletes shadow copy backups in order to make data delivery more difficult.[6] When the victim pays the ransom, the attacker promises to decrypt the files. Besides the extortion, attackers have also threatened to publicly expose victims' sensitive data.

What has become abundantly clear in 2021 was the burgeoning of ransomware supply-chain attacks. These attacks are designed to exploit trust relationships between an organization and external parties, including partnerships, vendor relationships, or the use of third-party software.

[5] "FBI Seized roughly $2.3 Million in Cryptocurrency tied to ransomware attacks, by CNN, December 1, 2021
[6] "Malware Families," Check Point Research



"A lot of those techniques of lateral movement across networks and targeting credentials and password spraying—all of these credential-based attacks end up in a fairly rudimentary toolkit for any country to use."[7]

Cryptojacking

Cryptojacking attacks install malware in a victim's computers, or injects malicious code into a victim's webpage to steal the use of computing and network resources to mine cryptocurrency, which is deposited in the attacker's exchange account. Attackers reap the rewards while victims pay for computing resources and electricity.

A recent example is the Glupteba botnet that since 2020 is estimated to have infected one million devices since 2020.[8] The botnet was instrumental to compromising thousands of people per day by installing coin miners on Windows PCs in attempts to steal login credentials and authentication cookies. It spread via Google ads, and per their researchers was tracked to an experienced cybercriminal group. In yet another vicious twist, some of the stolen credentials and credit card numbers were used to fund further malicious Google Ads.

Cryptocurrency hacks continue to proliferate in size and number. A United Nations report found North Korea's hackers stole $316 million through the breach of at least seven cryptocurrency exchanges in 2019 and 2020.[9] Another $400 million heist in 2021 saw perpetrators not immediately convert stash to regular currency to take advantage of rising profits.

[7] "Reduce the 'blast radius' in credential attacks, Krebs advises," by Stephanie Kanowitz, GCN, November 8, 2021

[8] "Google Disrupts Glupteba Cryptojacking Botnet With Removal of Hosted Ads, Documents and Accounts, & Notifications to Web Hosts," by Scott Ikeda, CPO, December 15, 2021

[9] "North Korea stole a record $400 million in cryptocurrency last year, researchers say," by Kevin Collier, NBC News, January 13, 2022

Maturing of cybercrime as a service

Ransomware as a Service (RaaS), botnets for rent, malware development, stolen personal data and other cybercrime tools and services are available on demand through the Dark Web. Criminal to Criminal (C2C) services let money flow within criminal gangs by making cybercrime easy to do and much less expensive than creating cyber attacks from scratch.

Don’t forget about identity theft

Identity theft is still a real threat. The Aite Group reports that identity theft cost the world $712.4 billion in 2020. It includes credit-card fraud, government-benefits fraud, loan or lease fraud, employment or tax fraud, phone or utilities fraud, and bank fraud.[10]

Identity thieves can and will play both ends against the middle, stealing user data from organizations through phishing, malicious www sites, code injections, malware, and other hacking techniques. Attackers also steal identity data and credentials directly from users through banking Trojans and other spyware spread by botnets, and phishing campaigns as well as drive-by downloads from infected and imitation websites.

These two examples demonstrate how cyber criminals steal or compromise computing resources to carry out multistage attacks. However, several types of cybercrime depend on compromising the computing and network assets of their victims for direct moneymaking schemes. In both cases, victims pay for computing power, electricity, cooling costs, and other associated data center costs. Or, potentially even more expensive, the victim pays for criminals to use virtually unlimited cloud computing.

[10] Lyle Daly, Identity Theft and Credit Card Fraud Statistics for 2021, The Ascent, Aug. 26, 2021. https://www.fool.com/the-ascent/research/identity-theft-credit-card-fraud-statistics/

Conclusion

Cyber attacks come through multiple vectors that can compromise and impact virtually every component within victims' computing and network environments. The most practical, economically sensible way to protect your organization from being the next victim is to deploy a consolidated security architecture that provides complete coverage of your end points, cloud resources and data center environments, uses preventative threat prevention with artificial intelligence to exclude attacks before they do damage; and streamlines monitoring, administration, and management to reduce the costs and complexity of security.

To learn more about consolidated security architecture, visit Check Point Infinity.

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

© 2022 Check Point Software Technologies Ltd. All rights reserved.