Secureworks®

WHITE PAPER

Keeping Tabs on a Constantly Evolving Threat Landscape

Criminal threat actors aren't just developing their tactics and techniques; they are updating their 'business' strategy too

What does your organization have that others might want? For most companies that fall victim to cybercrime, the answer to that question is money.

Approximately 80% of Secureworks® incident response engagements are in response to system attacks from cybercriminal threat actors (the remainder splits between company insiders doing something they shouldn't, and government-sponsored threat actor attacks).

When we talk about how the threat landscape is evolving, we often focus on technical topics – new zero-day exploits, a previously unseen malware variant, or different types of tactics, techniques, and procedures (TTPs).

However, some of the biggest changes happen in another aspect of cybercriminal activity – the threat actors' strategy.

To Find the Strategy, Follow the Money

Cybercriminal operators are adopting strategies often seen in the legitimate business world to increase return on investment (ROI) and operational efficiency. They respond to external market forces and innovate in order to elevate how 'compelling' their 'product' appears, and to ensure longevity and resilience to those market forces.

Over recent years, criminal threat activity has pivoted from using banking trojans to gain access to victim bank accounts, to commodity ransomware, to post-intrusion ransomware. We've seen it turn to cryptomining when cryptocurrency prices were high and reducing that specific activity when prices plummeted. Each move is designed to grow and maximize the payout.

Of course, earlier threat types don't go away – the most widespread banking trojan, Zeus, first seen in 2007, has spawned multiple variants, a recent example being Zloader in 2020. Emotet, Trickbot, and Danabot are still in active use. Threat actors continually refine malware to evade detection and deliver ever more sophisticated payloads. Organizations face the challenge of monitoring for all generations of threats: legacy, developing, and new.

Clearly, these 'product' developments are strategic as well as technical. Offering an as-a-service malware product for other threat actors to use is less effort-intensive than targeting individuals' bank accounts. Demanding ransoms in cryptocurrency removes the requirement for money laundering effort and expense. Post-intrusion ransomware enables bigger ransomware demands than commodity ransomware.

New Business Models

In parallel, business models and practices are changing. Not only did the number of cryptomining incidents rise and fall in direct correlation with cryptocurrency prices, but other evolution and diversification is taking place too. Cloud environments are being targeted for mining because the potential computational power is greater and so is the

resulting return. Cryptominers are also being dropped alongside information stealers and other sorts of threats.

'Traditional' banking malware such as Emotet, Dridex, and TrickBot has evolved to become modular. It has developed the ability to send out spam to a compromised user's mail contacts. It has branched out to deliver additional malware payloads.

Many malware operators have shifted to a cloud business model, offering malware-as-a-service – one of the first to do this was GandCrab. Some clearly work standard business hours, including taking lunch breaks.

Affiliate models allow operators to recruit junior partners who choose and exploit their own targets to install the operator's malware. Once the malware is communicating with their infrastructure, the operator takes over from the affiliate and both partners share the proceeds. Some of those actors have branched out into ransomware or have developed close business relationships with others who do – Dridex with BitPaymer, TrickBot with Ryuk.

In fact, ransomware is a field where this element of change is particularly apparent. Ransomware-as-a-service operators make money by taking a percentage of their customer's earnings. They potentially broaden their reach, while their customers avoid the burden of developing their own malware. Examples include LockBit and Smaug.

The move to exfiltrating data before encryption allows multiple or alternative revenue streams from separate payment demands – for decrypting the data and/or for not publishing it. Ransomware operators using this Name and Shame tactic include Maze, Doppelpaymer, REvil, and Nemty.

Multi-victim or repackaging attacks allow ransomware operators to extort ransoms from not just the data processor, but also organizations that are data subjects of the victim. REvil has also moved towards auctioning data to the highest bidder, rather releasing it for free if the victim does not pay.

Forming consortiums or cartels is a further strategic approach. One example is GOLD VILLAGE, the operators of Maze Ransomware, with LockBit and Ragnar Locker.

In total, these developments have driven the value of ransom demands sharply up. In 2018, an average ransom demand for a commodity, single-host ransomware attack stood at around $6,000 USD. In early 2020, the average stood at around $111,000 USD[1] and the general trend remains upwards.

Like most economic actors, criminal threat actors are interested in ROI. They view themselves as organized, adaptive, money-making enterprises. The operator of Maze ransomware recently said of their collaboration strategy: "We treat other groups as our partners, not as our competitors. Organizational questions is [sic] behind every successful business."[2]

$6,000 USD

was an average ransom demand for a commodity, single-host ransomware attack in 2018.

$111,000 USD

is the average stood in early 2020.

[1] Coveware, Ransomware Payments Increase In Evolving Distribution of Enterprise Ransomware Variants

[2] Bleeping Computer, Ransomware gangs team up to form extortion cartel

Secureworks®

Tracking and understanding these changes doesn't just help make sense of how the criminal threat landscape has evolved over the last ten to fifteen years, it provides guidance for organizations in protecting themselves. It's also something that external threat intelligence providers are well placed to do.

However, we should shy away from treating these cybercriminals as a homogenous group. Some have switched to ransomware, while many have not. Some have learned new skills, but others have just evolved what they've always done and always been good at. What has changed potentially is the increasing collaboration between these groups and others, once again with the intent of maximizing ROI.

The operator of Maze ransomware recently said of their collaboration strategy: "We treat other groups as our partners, not as our competitors. Organizational questions is [sic] behind every successful business."

The Challenge to Organizations

These criminal enterprises are operating as businesses, making decisions to increase ROI, expand capabilities and ensure resilience to outside forces, just like legitimate businesses do, but unencumbered by regulatory oversight and public opinion.

For organizations, the challenge is to either entirely prevent cyberattacks, or to identify and stop intrusions at an early stage. Two things make that easier. One is a clear understanding of the threat landscape and the threat operator playbook – what threat actors are doing and how they are doing it. The other is comprehensive visibility of the organizational environment from modern solutions and services like endpoint monitoring systems.

Both are more achievable with the right external threat intelligence supplier, one that focuses both on technical aspects of the threat landscape such as tools, tactics, techniques, and procedures, and on the way in which threat actors are changing their behavior and strategies. The result is guided intelligence and insight, customized to the needs of the organization, to make it actionable and relevant.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp