WEBINAR SUMMARY

April 8, 2021

black hat®

It's not FINished: The Evolving Maturity in Ransomware Operations

Mitchell Clarke, Principal Incident Response Consultant, Mandiant
Tom Hall, Principal Incident Response Consultant, Mandiant
Joe Slowik, Senior Security Researcher, DomainTools

KEY TAKEAWAYS

- Attackers are targeting specific organizations with ransomware.
- REvil: RaaS provides attackers automation and scalability.
- QAKBOT and DopplePaymer are a ransomware partnership.
- As the ransomware problem grows, it is becoming a boardroom risk.

in partnership with

DOMAINTOOLS®

OVERVIEW

Ransomware attacks have evolved beyond opportunistic phishing and hidden web exploits; they are now targeted attacks against organizations that can completely shut down operations. Ransomware is also becoming more difficult to detect and stop as intrusion tactics continuously improve.

Threat actors are also streamlining attacks, developing sleek ransomware-as-a-service (RaaS) platforms, and creating partnership models. These tools and models are being used to generate malware, communicate and negotiate with victims, and in some cases, handle payment processing and decryption delivery, simplifying—and improving the profitability of—the entire ransomware process for the attacker.

CONTEXT

Mitchell Clarke, Tom Hall, and Joe Slowik discussed how ransomware operations are evolving and what organizations need to be prepared for in the future.

KEY TAKEAWAYS

Attackers are targeting specific organizations with ransomware.

Ransomware operations have shifted from self-propagating malware, like WannaCry and NotPetya, to attacks manually triggered by a human attacker. While some attacks are still "spray and pray," taking advantage of widespread vulnerabilities, many are now targeted at specific organizations, following an advanced persistent threat (APT)-style intrusion life cycle.

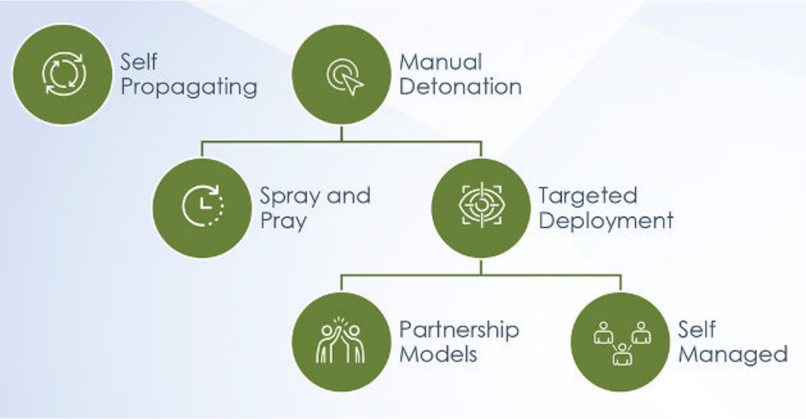
Table 1: Ransomware attackers are using APT-style intrusion

APT attack	Ransomware adds to the APT attack
– Attacker has domain access to the organization's environment – There are multiple persistence methods within the environment, preventing the organization from removing the attacker's access – The attacker has probably stolen business-sensitive data	– The entire IT infrastructure is down – The business is unable to function without access to the IT infrastructure, files, data, etc.

> Ransomware operators have learned that if they behave like APT intruders and they go for longer, more persistent intrusion, they can bring the business to a complete halt.
>
> *Mitchell Clarke, Principal Incident Response Consultant, Mandiant*

Bad actors are using both partnerships and self-managed models within targeted ransomware deployments. Partnerships use platforms from other operators, while self-managed attacks are handled end-to-end by a single bad actor or organization.

Figure 1: Ransomware operations are tending toward manual detonations and targeted deployments

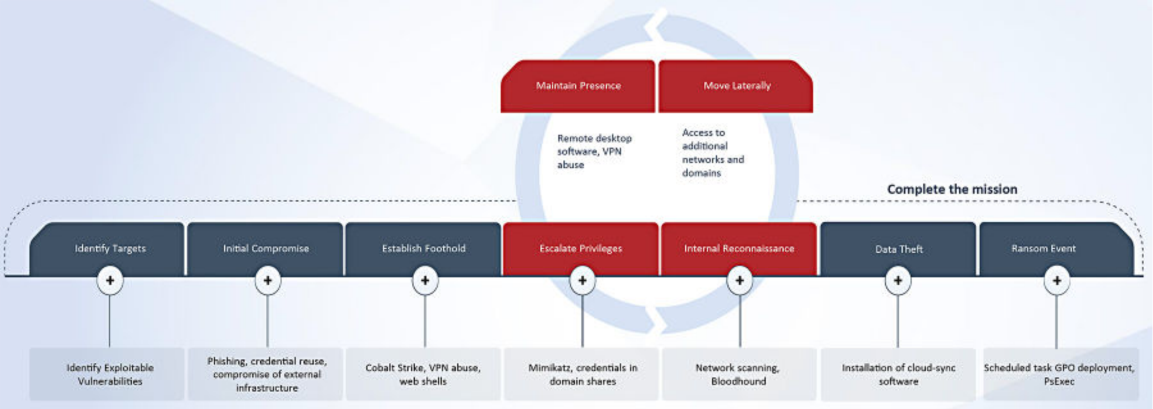


REvil: RaaS provides attackers automation and scalability.

First seen in 2019, REvil is a RaaS model that offers affiliated attackers a platform for malware generation, a random demand and payment service, victim communications, and cryptocurrency laundering. Affiliates receive an estimated 60% to 75% of payouts from their attacks using the REvil platform, depending on performance, with the rest of the payouts going to REvil's operator, UNKN.

The tradecraft and implementation of phases in the attack life cycle vary by attacker, especially when implementing the compromise and establishing a foothold.

Figure 2: The REvil attack life cycle


Maintain Presence
Move Laterally
Remote desktop software, VPN abuse
Access to additional networks and domains
Complete the mission
Identify Targets
Initial Compromise
Establish Foothold
Escalate Privileges
Internal Reconnaissance
Data Theft
Ransom Event
Identify Exploitable Vulnerabilities
Phishing, credential reuse, compromise of external infrastructure
Cobalt Strike, VPN abuse, web shells
Mimikatz, credentials in domain shares
Network scanning, Bloodhound
Installation of cloud-sync software
Scheduled task GPO deployment, PsExec

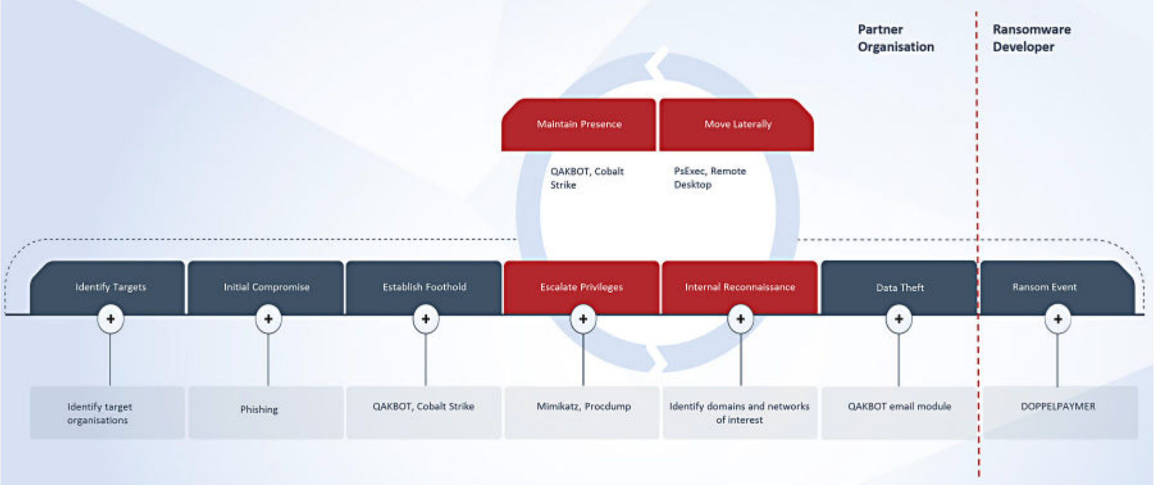
The initial compromise is usually done by mass exploitation of high-profile vulnerabilities for the internet-facing infrastructure. While some attackers will move into ransomware deployment immediately after compromise, others will gain a foothold in the network, waiting as long as four months to deploy ransomware, often because they have a backlog of targets to attack.

Attackers often steal sensitive data from organizations, giving them more leverage for payout once the ransomware is deployed. They then deploy the Sodinokibi ransomware that REvil uses, deleting file backups, archives, and virtual machine snapshots, and begin the encryption process, locking users and organizations out of systems and data.

QAKBOT and DopplePaymer are a ransomware partnership.

In 2020, organizations began seeing attacks using the banking Trojan QAKBOT, partnered with ransomware, especially DopplePaymer. QAKBOT is used to provide access to a compromise environment, while the ransomware providers focus on negotiations and payment.

Figure 3: The QAKBOT and DopplePaymer partnership in the ransomware attack life cycle



In early 2020, QAKBOT campaigns were seen using unsophisticated phishing scams to gain initial access to systems. The Trojan then creates a back door that allows the attacker to establish a foothold in the system and steal data. DopplePaymer then removes access to systems and encrypts files.

As the ransomware problem grows, it is becoming a boardroom risk.

Ransomware continues to grow relatively unchecked, as the pressure from law enforcement remains minimal and the rewards to attackers increase, including payouts, the number of victims, damage that can be done to organizations, and extortion opportunities for stolen data. This is driving senior business executives in organizations around the world to recognize ransomware is a significant risk to their businesses and to take action.

> It's getting across to senior stakeholders that ransomware is a big issue. It's fixable, but there has to be a real effort to put more spend on some of the outdated IT systems and really invest in security.
>
> *Tom Hall, Principal Incident Response Consultant, Mandiant*

These attacks have evolved beyond opportunistic targeting of individuals via phishing and exploit kits hosted on compromised websites; they are targeting organizations based on payout potential and moving into critical infrastructure, such as hospitals.

> We have seen increasingly bold operations. From 2019 to the present, we've seen ransomware operators targeting pipelines, hospital systems, and similar elements of critical infrastructure.
>
> *Joe Slowik, Senior Security Researcher, DomainTools*

Organizations need to be ready to combat an anticipated future of ransomware attackers brazenly targeting victims, increasing disruption to businesses, and potentially becoming a cover for state actors.

The anticipated future of ransomware	
Brazen targeting	– Continued expansion into critical infrastructure – Sensitive targets deliberately chosen; this has been seen with industrial control system-focused ransomware variants
Increased disruption	– Increasing the desire to expand disruption to force ransom payment – The likelihood for “knock on” effects, where an event designed for monetization purposes also results in logical or physical disruption to the business
Possible cover for state actors	– An active criminal disruptive ransomware space opens up room for other actors, especially without meaningful pushback from legal authorities or state authorities – Potential for a “wipers” transition to ransomware with no intent to enter negotiation or accept payment of ransom

BIOGRAPHIES

Mitchell Clarke

Principal Incident Response Consultant, Mandiant

Mitchell Clarke is a Principal Incident Response Consultant for Mandiant United Kingdom and Ireland. He specializes in providing enterprise-scale response operations for clients facing sophisticated network intrusions by determined attackers. Mitchell is well practiced in leading both large and complex response operations for multinational organizations as well as tightly focused response operations for highly specialized organizations protecting critical intellectual property or sensitive information. Mitchell has led organizations across multiple industries in responding to breaches by adversaries ranging from well-resourced and stealthy nation-state sponsored espionage threat groups to highly motivated cybercriminals seeking to extort or ransom victim organizations.

Tom Hall

Principal Incident Response Consultant, Mandiant

Tom Hall is a Principal Incident Response Consultant in Mandiant’s UK team, and European Incident Response Function lead. As part of the Incident Response team, Tom provides services to clients when a breach occurs and has worked on Incident Response engagements globally with Mandiant since 2015. Tom has been responsible for leading and assisting organizations that involved advanced targeted threats and works closely with colleagues on new methods to proactively identify threats using new methodologies.

Joe Slowik

Senior Security Researcher, DomainTools

Joe Slowik has over a decade of experience across multiple cyber disciplines. From work in the US Navy, to the US Department of Energy and Los Alamos National Laboratory, to industrial control security company Dragos, Joe has covered multiple facets of cyber intrusions and critical infrastructure defense. As a Senior Security Researcher at DomainTools, Joe continues his work tracking state-sponsored and criminal threats to enterprises with an emphasis on critical infrastructure and related targets.