MANDIANT®

The Evolving Maturity in Ransomware Operations

A Black Hat Europe 2020 Whitepaper

December 2020

Mitchell Clarke and Tom Hall

ABSTRACT

Ransom demands are becoming larger, attackers smarter, and intrusions longer. Ransomware threat actors are hitting European and global companies hard with more effective ransomware deployment resulting in devastating impacts to victim organisations. When they strike, their ransomware deployments are more complete, more effective, and they are crippling many organisations to the point where there is often no clear path back to business.

This whitepaper outlines different operating models in use by ransomware threat groups during 2020, specifically ransomware as a service and partnership models. Ransomware as a service involves multiple threat actors that make use of a central shared platform to automate and streamline repetitive processes encountered during ransomware operations.

Partnership models involve handover between threat actors, often separating initial intrusion and privilege escalation from mass deployment of ransomware extortion of victims. This allows threat actors to specialise in specific stages of an intrusion lifecycle, enabling them to operate with increased efficiency and effectiveness.

This whitepaper reviews tradecraft that ransomware threat actors have employed across Europe in 2020. This includes how ransomware crews leverage high-profile critical vulnerabilities to gain footholds in multiple victims' networks and return weeks or even months later to leverage those footholds into full-scale ransomware deployments.

INTRODUCTION

The ransomware industry has continued to evolve during 2020. Ransomware threat actors are increasingly conducting full-scale network intrusions similar to those seen in nation-state Advance Persistence Threat (APT) or financially motivated criminal intrusions. Full-scale network intrusions allow threat actors to deploy ransomware across the entirety of victim organisations, often with devastating consequences.

Historically, ransomware has often been deployed opportunistically or in a non-targeted manner where a handful of systems or small network segments were infected. Several global high-profile, high-impact ransomware infections in the past, such as WannaCry or NotPetya, were non-targeted events and were self-sustaining with no interaction with attackers after initial malware deployment.

Since the days of WannaCry and NotPetya, the ransomware industry has evolved as threat actors chase ever-increasing ransom pay-outs. Threat actors have matured from opportunistic ransomware deployment to become co-ordinated professional organisations with a focus on sustained traditional network intrusions in order to be best placed to deploy ransomware as widely as possible across victim environments. This approach to sustained intrusion and comprehensive ransomware deployment can take days, weeks, or months.

By deploying ransomware to the entirety of a victim network, threat actors are applying maximum pressure on victim organisations to pay the demands set by the attackers. Mass ransomware deployments responded to by Mandiant are increasingly threatening business continuity and leaving victims with a decision between paying ransoms and being unable to continue to trade or operate.

Additionally, ransomware threat actors are also increasingly stealing victim data and threatening to publicly release stolen data thereby adding extra pressure to victim organisations.

With this continued evolution, ransomware attackers have become more effective and increasingly efficient. Mandiant sees this play out in two different ransomware models:

1. Ransomware as a Service – which features automation and scale. This paper profiles REvil, a threat group made up of individual affiliates using a common ransomware platform.
2. Partnership Models – where threat actors focus on different parts of an intrusion, such as traditional network compromise, while others focus on ransomware deployment, data theft and extortion. This paper profiles QAKBOT and DOPPELPAYMER groups, who perform different stages of the intrusion and handoff victims between them.

REVIL AND SODINOKIBI

Overview

REvil refers to a collection of threat actors who use a common ransomware as a service platform created by a threat actor that goes by the name of UNKN or Unknown. UNKN began advertising for affiliates to join the platform in mid-2019 and since then, many threat actors have joined REvil, gaining access to the automation and process benefits that the platform provides.

UNKN advertises that affiliates can retain 60 to 70 percent of ransoms in exchange for use of the platform. Affiliates that perform well and obtain large and/or regular ransom payments will receive higher pay-outs while poorly performing affiliates will receive less and can potentially be removed from the platform.

This type of ransomware operation is known as an affiliate model. While each threat actor within the program gains access to the SODINOKIBI ransomware used by the group, each affiliate operates independently.

This leads to REvil intrusions and SODINOKIBI ransomware deployments to vary widely in terms of tradecraft and targeting as each threat actor operates in isolation.

REvil tradecraft described in this whitepaper is an amalgamation of multiple individual affiliates.

Ransomware as a Service Model

Ransomware as a service involves use of a central platform which automates and streamlines business processes that are common to most ransomware intrusions. Threat actors have created these platforms to reduce operator-effort required for repetitive and common tasks to increase both scale and pace of operations while also improving the effectiveness of processes.

REvil's ransomware as a service platform provides affiliate threat actors with the following services:

- Malware provision and generation, enabling threat actors to generate new and unique malware samples per victim or operation
- Ransom demands, enabling threat actors to centrally set and manage a ransom amount for the targeted victim organisation
- Payment information, removing the burden of communicating and managing cryptocurrency wallet details for each ransom operation
- Victim communications, allowing the attacker to negotiate the ransom amount and to share stolen files to prove to victims that threat actors have successfully exfiltrated data from victim networks
- Cryptocurrency laundering, which reduces the attribution of cryptocurrency profits paid to affiliate threat actors

The REvil ransomware platform provides automation, efficiency, and increased effectiveness during ransomware operations.

Development of ransomware as a service platforms can be compared to the scale-out and scale-up of legitimate businesses facing rapid growth opportunities.

Tradecraft

Whether an intrusion is performed by a nation-state sponsored APT group, a criminal group, or a ransomware group, threat actors must step through common phases of an intrusion lifecycle, shown in Figure 1, to be able to achieve their objectives.

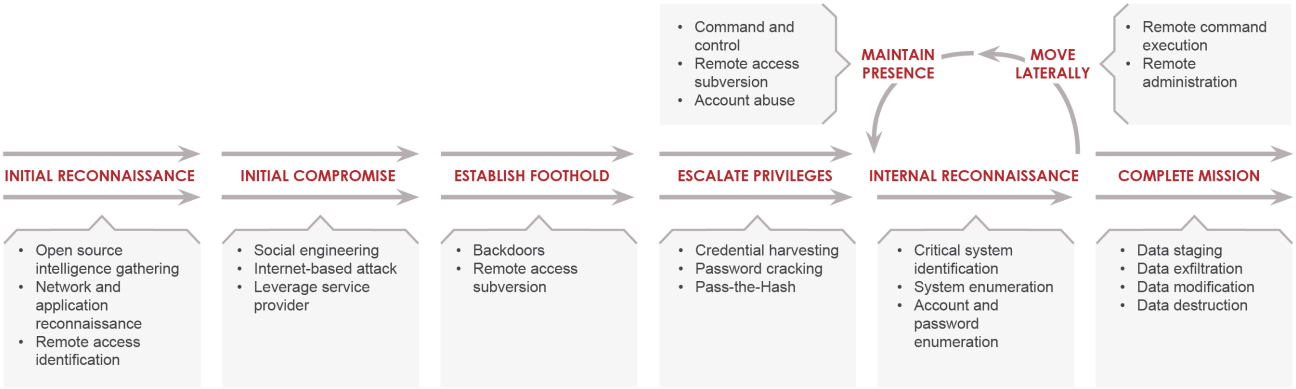

Figure 1: An example targeted attack lifecycle for a full-scale network intrusion

REvil tradecraft varies between individual threat actors. Broadly, however, REvil threat actors have performed APT-like intrusions during 2020 which are full-scale network intrusions that can span days, weeks, or even months. REvil threat actors are employing tradecraft similar to that of APT or financial crime groups to gain the highest level of privilege within victim organisations. This privilege, combined with effective organisation-wide network reconnaissance and lateral movement, allows REvil attacker to launch devastating SODINOKIBI ransomware deployments often impacting the entirety of a victim network.

These prolonged intrusions with APT-like tradecraft can have devastating consequences for victim organisations when ransomware is deployed, often leaving them without the ability to perform basic day-to-day business operations.

Initial Compromise

REvil threat actors are leveraging high-profile and high-impact vulnerabilities of internet-facing edge devices to mass-exploit many victims simultaneously.

Vulnerabilities in edge-devices are attractive for REvil threat actors as they are exposed to the internet by design and provide a method of initial access to the victim corporate networks.

By conducting mass-exploitation of vulnerable edge devices, REvil attackers are able to gain access to multiple victim organisations. REvil threat actors then likely triage these accesses to prioritise organisations the actors believe will be more likely to pay ransoms.

During 2019, many vulnerabilities were discovered in internet-facing edge devices. REvil exploitation of these well-known vulnerabilities often occurred months after vulnerability disclosure and patch release. Vulnerabilities exploited in edge-devices by the REvil threat actors include:

- VPN devices
- Web services
- Remote desktop appliances
- Internet-facing remote desktop services

Establish Foothold

Due to the high number of vulnerable devices exposed to the internet, REvil threat actors who conduct mass-exploitation will often have a backlog of victims to triage and prioritise. Some of these threat actors will progress intrusions from initial access to a surer setting by establishing additional remote access mechanisms to victim environments. These methods may include:

- Use of Cobalt Strike BEACON malware

- VPN abuse
- Installation of web shells on internet-facing victim web servers

Escalate Privileges

After establishing a foothold to victim organisations, REvil threat actors will use a multitude of privilege escalation techniques in order to gain administrative access to victim environments that are similar to those used during APT, financial crime, or red team intrusions. These include but are not limited to:

- Mimikatz and other password dumping utilities
- ProcDump to obtain process memory of the Windows Local Security and Authorisation Sub-system (LSASS)
- Passwords for privileged local administrator or domain accounts stored as *cpassword* objects within legacy group policy preferences
- Credentials stored within domain shares, for example, hard-coded credentials within corporate PowerShell scripts
- Credentials stored in user profiles, such as text files or Excel spreadsheets

Internal Reconnaissance

REvil threat actors are performing comprehensive internal network reconnaissance in an attempt to fully understand victim networks and maximise the effectiveness of ransomware deployments. REvil threat actors are using network scanning and domain enumeration tools to discover:

- Additional corporate networks
- Additional Active Directory domains

Tools employed by REvil attackers include:

- Advanced IP Scanner
- SoftPerfect Network Scanner
- Bloodhound, an open-source domain enumeration tool
- Built-in Windows commands to gather Active Directory information

Move Laterally

Once REvil threat actors discover and gain familiarity with victim networks, they will move laterally to network segments and systems of interest using stolen administrative credentials and using multiple tools and techniques, such as:

- WMIExec (remote execution tool)
- SMBExec (remote execution tool)
- CrackMapExec (remote execution tool)
- PsExec (remote execution tool)
- RDP (legitimate Microsoft remote desktop service)

Maintain Presence

In order to retain access to additional network segments or environments within victim organisations, REvil threat actors will often establish additional persistent backdoors or abuse legitimate remote access solutions in preparation for organisation wide SODINOKIBI ransomware deployment.

This provides the attackers with independent remote access to each targeted network segment.

Methods of persistence vary between individual REvil affiliates, however Mandiant has observed repeated use of the following persistence methods:

- Installation of commercial/freemium internet remote desktop software
- Cobalt Strike BEACON
- Web shells installed on internet-facing victim web servers
- Continued VPN abuse using compromised credentials
- Continued abuse of remote desktop appliances using compromised credentials

Data Theft

Prior to deploying SODINOKIBI ransomware, REvil threat actors will often steal data from victim organisations.

Data theft is conducted prior to ransomware deployment to increase pressure on victim organisations to pay ransom demands. The REvil threat actors will threaten to publicly release stolen data, extorting victims and increasing pressure.

Methods of data theft used by REvil include:

- Compression and exfiltration of targeted data using malware deployed within victim organisations
- Installation of commercial cloud data synchronisation platform software to upload targeted data. Once installed, the commercial synchronisation software will upload targeted data to the cloud platform. The threat actors are then able to access victim data via the commercial cloud platform.

Ransomware Deployment

After gaining administrative access to domains and networks within victim organisations, the REvil attackers will prepare and deploy SODINOKIBI ransomware as widely as possible.

Prior to deploying ransomware, REvil attackers have been observed attempting to increase the likelihood of successful SODINOKIBI execution by disabling antivirus software across victim environments, usually by either:

- Accessing central corporate antivirus consoles using administrative credentials to disable antivirus across the entire victim estate
- Mass-deploying open-source administrative scripts that disable antivirus to individual systems within the victim estate.

After disabling antivirus software across victim environments, the most common method of SODINOKIBI ransomware deployment is the abuse of corporate Group Policy and unrestricted file shares:

1. The attacker will create file shares on victim domain controllers accessible to all users and systems within the targeted domain. The file shares are used to store SODINOKIBI ransomware binaries.
2. The attacker then creates a Group Policy Object in the default domain policy for all computers to create and execute a scheduled task. The scheduled task downloads and executes SODINOKIBI ransomware binaries from the open file shares created on targeted domain controllers.

3. When the computers within the targeted domain next update Group Policy, they create and execute the attacker-created scheduled task which in turn downloads and executes the SODINOKIBI ransomware.

After creating malicious group policy to deploy SODINOKIBI ransomware across a targeted domain, the REvil attackers will often use remote execution tools to deploy the SODINOKIBI ransomware to systems that have not updated Group Policy objects or have otherwise not been infected with ransomware. This action maximises the number of victim computers ransomed by the attacker and increases the impact to victim organisations.

Once executed, SODINOKIBI will encrypt files on infected computers and create ransom messages that guide victims to the REvil ransomware as a service platform for ransom negotiation and payment.

QAKBOT AND DOPPELPAYMER

Partnership Model

During 2020, Mandiant responded to DOPPELPAYMER ransomware deployments across Europe and globally where initial access was achieved through widespread use of QAKBOT malware.

In contrast to REvil's affiliate model where individual threat actors are responsible for end-to-end intrusions from initial access to ransomware deployment, QAKBOT and DOPPELPAYMER employ a partnership model where one threat actor is responsible for initial access, privilege escalation, and lateral movement which is then passed to another threat actor for DOPPELPAYMER ransomware deployment.

QAKBOT Modules

QAKBOT is often delivered to victims via unsophisticated, yet effective, spear phishing campaigns. QAKBOT is a modular backdoor originally used as a banking trojan and has since been leveraged as a precursor to DOPPELPAYMER ransomware deployment.

QAKBOT is a modular backdoor that allows for individual capabilities to be deployed to infected systems. Key modules include:

- **Email Staging Module:** A standalone module independent from other QAKBOT modules that steals email from a local Outlook instance using MAPI connections. Email data is compressed, base 64 encoded, and sent to a hardcoded command and control server.
- **Cobalt Strike Module:** Loaded using one of two methods:
    - By executing a file dropped using the malware
    - Via a pre-configured DLL as a QAKBOT module
- **Web Inject Module:** Traditional banking trojan functionality that targets JavaScript loaded in Northern American banking organisation websites.

After infecting organisations with QAKBOT malware and gaining privilege within targeted environments, threat actors will hand access to QAKBOT backdoors to other threat actors using DOPPELPAYMER to mass-deploy ransomware across victim networks.

DOPPELPAYMER Deployment and Execution

After obtaining access to victim networks using existing QAKBOT infections, threat actors will deploy DOPPELPAYMER ransomware using techniques similar to other ransomware operators:

- PsExec

- Background Intelligent Transfer Service (BITS) Jobs
- Scheduled Tasks

Once executed, DOPPELPAYMER ransomware performs the following actions:

- Enumerate all local users of a system and change the password for each user. This prevents victims from logging into infected systems. The password is generated by combining a pre-configured string with an MD5 hash of the system name, for example:
    - Preconfigured string: TtXtE9n3
    - Computer name hash: 384DFCCEE8DB9F89ED2859E3F32F6AF5
    - Full password: TtXtE9n3&384DFCCEE8DB9F89ED2859E3F32F6AF5
- The ransomware will then copy legitimate services and replace them with a copy of itself in order to establish persistence:
    - **File:** <random>.exe
        - Path: %APPDATA%\<random>.exe
        - Note: Copy of DOPPELPAYMER binary
    - **Service:** <random_service>
        - Path: %WINDIR%\system32\<random_service>.exe
        - Note: Ransomware Service
    - **Service:** <random_service>-1
        - Path: %WINDIR%\system32\<random_service>.exe-1
        - Note: Backup of Service
- The ransomware will then modify the boot configuration database of the infected system in order to disable start up repair and to execute the ransomware during safe boot.
- The ransomware will also modify group policy to display a ransom message prior to logon which directs victims to the threat actor's TOR website for ransom negotiation and payment.
- Finally, after rebooting the system, the DOPPELPAYMER ransomware will begin encrypting files on the affected system and will create ransom notes to direct victims to the threat actor's TOR website.

CONCLUSION AND OUTLOOK

With increased impact and visibility, the threat of ransomware has widely become a boardroom issue, now placing highly on corporate risk registers. Enterprise-wide ransomware infections are becoming business-halting events, with many organisations facing loss of revenue and critical impact to business continuity.

Ransomware continues to be a growing problem beyond 2020, both in Europe and globally. During 2020, the following key metrics for ransomware intrusions have increased:

- Ransom amounts
- Number of victim organisations
- Damage incurred by increasingly effective organisation-wide ransomware deployments
- Extortion for stolen data

With ransom profits assumedly being at an all-time high, ransomware threat actors have continued incentive to automate operations, gain additional operators, partners, and/or affiliates, as well as to scale platforms to allow attackers to infect more organisations with increasing efficiency and devastation.

Increased impact to business continuity may increase or better focus information security spending and encourage organisations to secure environments and improve security baselines. While this may protect organisations from tradecraft currently employed by ransomware threat actors, it is likely that attackers will improve tradecraft in a continuous manner as seen in APT and financial crime threat actors.

While ransomware intrusions have been highly effective during 2020, organisations can protect themselves and prevent these intrusions by focusing information security budgets on improving security programs and baselines including:

- Vulnerability management programs, ensuring critical vulnerabilities for internet facing infrastructure as well as critical internal privilege escalation vulnerabilities are patched as soon as possible
- Ensuring networks are actively and effectively monitored at scale for intrusions
- Implementing robust privilege access management solutions
- Ensuring critical or sensitive data is access controlled and cannot be easily exfiltrated
- Ensuring that robust backup solutions are in place and regularly tested to ensure that organisations are able to rapidly recover during a ransom event

FireEye, Inc.

601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About Mandiant Solutions

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®