Adversary Dossier: Ryuk Ransomware Anatomy of an Attack in 2021

advanced-intel.com/post/adversary-dossier-ryuk-ransomware-anatomy-of-an-attack-in-2021

AdvIntel April 16, 2021

- Apr 16, 2021
-
- 6 min read

By Vitali Kremez, Al Calleo, Yelisey Boguslavskiy

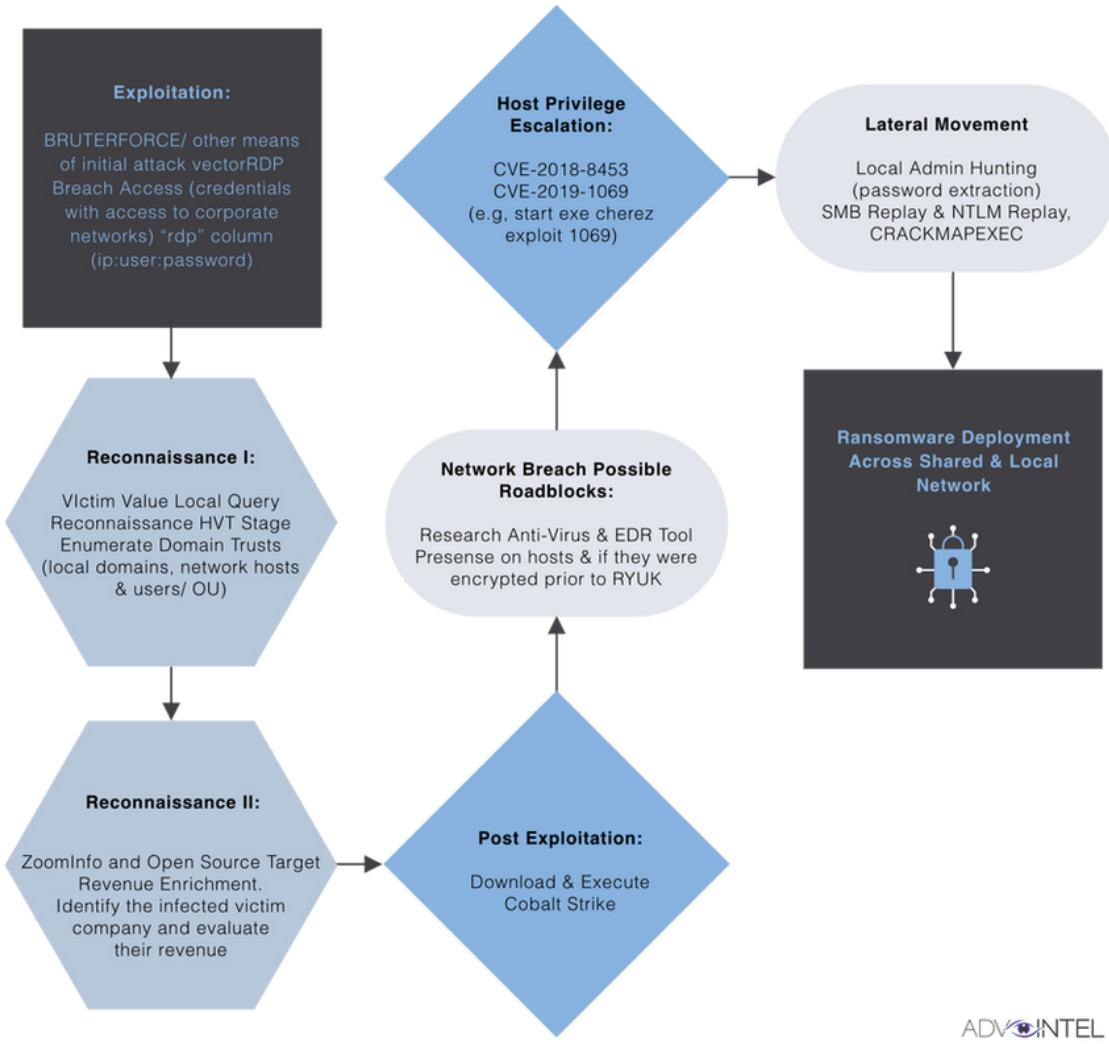
Ryuk ransomware infections have been observed since late 2018. Ryuk actors are constantly evolving the TTPs used in Ryuk attributed campaigns. Some of the most notable targets of these campaigns have been hospitals, government entities, and large

corporations. The Ryuk adversary group is widely considered to be one of the most successful and impactful targeting corporations and governments worldwide.

This report is an excerpt of the tactical report from the flagship Andariel platform produced by the subject matter expert team.

Background

This report illustrates some of the new and existing Tactics, Techniques, and Procedures (TTPs) of the Ryuk ransomware variants that Advintel has witnessed throughout their investigations in 2021.



Initial Attack Vector: RDP Brute Force / Other Means of Initial Attack Vector

Ryuk operators gain initial access to a network most often through two methods in 2021.

- Service-Based RDP Compromise
- Botnet-Based Malware Delivery

Advintel has noticed an overall increase of RDP compromise as the initial infection vector across Ryuk-attributed attacks. Threat actors have been observed in the wild employing large-scale brute force and password spraying attacks against exposed RDP-hosts to compromise user credentials.

Targeted phishing emails coupled with the support service center calls such as "BazaCall" have also been observed as an initial infection vector in many Ryuk-attributed attacks. This weaponized document will have instructions that tell the user to “enable content” which will

activate a macro and enable the document to download a malicious payload through a PowerShell script that is executed through a command prompt.

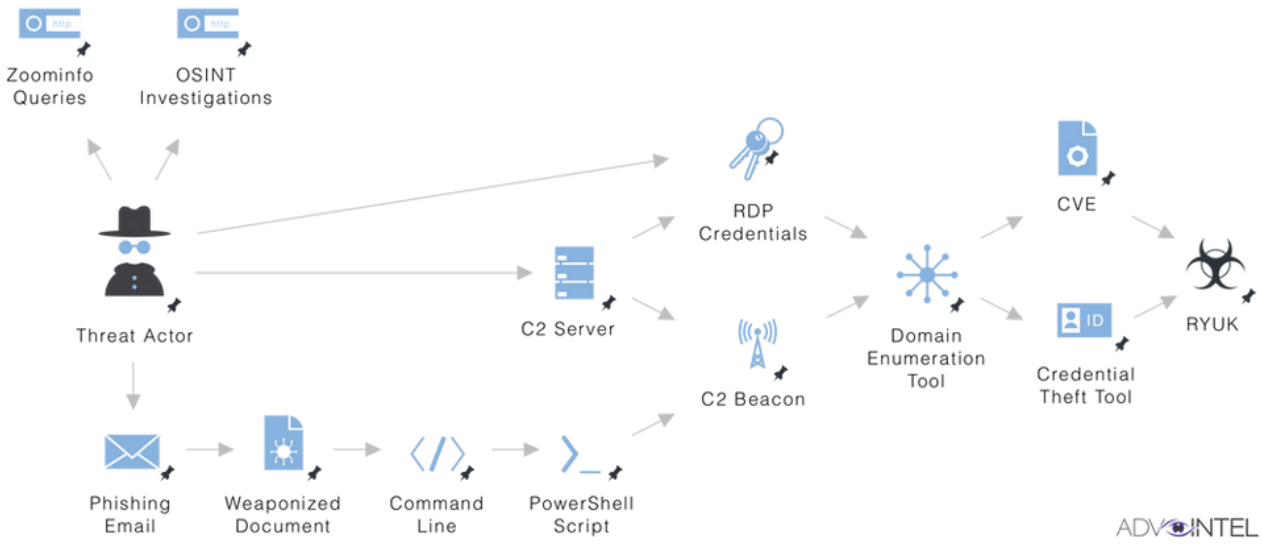


Figure 1. Ryuk Kill chain. (Source: Advintel)

Reconnaissance I: Victim Value Local Reconnaissance Stage

Once a foothold has been established Ryuk operators will attempt to enumerate domain trusts such as local domains, network shares, users, and Active Directory Organization Units. During this stage, the actors attempt to gather information about the organization to determine what resources within the infected domain are of value to perpetrating the rest of the attack. Bloodhound and AdFind have become popular tools used by actors trying to enumerate active directory information within an infected domain.

Reconnaissance II: ZoomInfo and Open Source Target Revenue Enrichment

Advintel has observed actors conducting OSINT research related to the compromised host domain to identify the infected victim company and evaluate their revenue. Ransomware operators use the total annual revenue of the victim's company to assess what the ransom amount will be. Specifically, actors have been observed searching across services such as ZoomInfo to retrieve information about the victim company such as technologies used, recent mergers and acquisitions, corporate hierarchies, personnel, and various other elements of data related to the company that may be of value to their operations.

Post-Exploitation: Cobalt Strike as Golden Standard Tool

After infection, Ryuk operators utilize Post-Exploitation toolkits such as *Cobalt Strike* to conduct further reconnaissance and operation.

Network Breach Possible Roadblocks: Anti-Virus & Endpoint Detection Response Bypass

Ryuk operators will utilize information collected by bot scans and their own scans to gain information about anti-virus (AV) and Endpoint Detection Response (EDR) tools present on hosts before formulating their attack. It is worth noting that operators will leverage OSINT methods and communication with other threat actors to gain information on the AV and EDR systems present in the networks that they are attacking especially if a network has been previously compromised the information obtained from the attack can be shared between threat groups. Once the operators successfully compromise a domain administrator account, they will work to disable AV and EDR services.

Some of the more sophisticated and novel red teaming techniques used to target and bypass EDR and protection tools:

- Hunting for a local IT administrator with access to EDR software and leveraging a PowerShell tool "**KeeThief**.**ps1**" to extract administrator credentials for EDR software from popular KeePass password manager
- *Allows for the extraction of KeePass 2.X key material from memory, as well as the backdooring and enumeration of the KeePass trigger system.*

*Deploying **portable Notepad++** version to run PowerShell scripts on the host system to bypass PowerShell* executionrestriction. The portable Notepad++ includes PowerShell version1.

Host Privilege Escalation

Advintel has witnessed two new TTPs relative to Ryuk ransomware campaigns that organizations should monitor closely as a means of detecting infections within their domain.

CVE-2018-8453

CVE-2018-8453 is an elevation of privilege vulnerability in Windows when the win23k.sys component fails to properly handle objects in memory. The exploitation of this vulnerability allows an attacker to run an arbitrary kernel with read/write privileges.

CVE-2019-1069

CVE-2019-1069 is a privilege escalation vulnerability that leverages the way Windows Task Scheduler handles saved tasks. Task Scheduler stores tasks as files in two locations, C:\Windows\Tasks and C:\Windows\System32\Tasks. If an RPC client modifies a task using the service in the C:\Windows\Tasks location when modifications are saved the task will be migrated to C:\Windows\System32\Tasks. When saving a task file, the Task Scheduler service will set ownership and full control of the file to the owner of the task. This process allows an attacker to perpetrate a hard link attack. Therefore, if an attacker manually places a file within C:\Windows\Tasks the attacker will be able to run this file with the highest level of privilege since the Task Scheduler service runs at the maximum level of privilege defined by the local machine.

Lateral Movement

Ryuk operators demonstrate high levels of sophistication in their abilities to gather information and move laterally within a network. Specific built-in tools of the Cobalt Strike toolkit have been witnessed being executed by actors including DACheck, and Mimikatz. A script “Invoke-DACheck” has been witnessed being used to identify domain admin accounts within the network. Actors will also use Mimikatz and LaZagne to collect passwords.

Advintel has recently witnessed Ryuk actors using CrackMapExec for local admin hunting and password extraction. CrackMapExec is a publicly available post-exploitation tool with a variety of enumeration, discovery, and brute force capabilities. It is likely that actors are using this tool to search for local admin accounts and then executing SMB and NTLM relay attack functions from this tool for authentication.

Ransomware Deployment

Once actors have successfully compromised a local or domain admin account, they distribute the Ryuk payload through Group Policy Objects, PsExec sessions from a domain controller, or by utilizing a startup item in the SYSVOL share.

Risk Mitigation Recommendations

- Detections for use of Mimikatz and PsExec execution within the network.
- Detections and alerts for the presence of AdFind, Bloodhound, and LaZagne within the network.

- Ensure all operating systems and software are up to date with the latest updates and security patches.
- Implement multi-factor authentication for RDP access.
- Implement network segmentation and controls to scrutinize SMB and NTLM traffic within the network.
- Routinely review account permissions to prevent privilege creep and maintain principle of least privilege.
- Routinely review Group Policy Objects and logon scripts.
- Update systems to prevent exploitation of CVE-2018-8453 and CVE-2019-1069.

Conclusion

Ryuk ransomware campaigns continue to evolve their TTPs to avoid detection and navigate throughout a network in 2021. Advintel continues to observe threat actors discussing new TTPs amongst themselves and will continue to monitor their communications to provide intel to prevent these campaigns from being perpetrated successfully.

Vitali Kremez *is CEO and Chairman of Advanced Intelligence LLC. Vitali specializes in researching and investigating complex cyberattacks, network intrusions, and data breaches. Over his government and private sector career, Kremez has made numerous groundbreaking findings into Eastern Europe's cybercrime underworld and has earned virtually every major certification available in the fields of IT, security, and digital forensics. Advanced Intelligence is an elite threat prevention firm. We provide our customers with tailored support and access to the proprietary industry-leading "Andariel" Platform to achieve unmatched visibility into botnet breaches, underground and DarkWeb economy and mitigate any existing or emerging threats.*

Al Calleo investigates ransomware incidents, data breaches, threat actor infrastructure, and performs research into emerging threats at Advanced Intelligence, LLC. He possesses a Bachelor's in Digital Media Production from SUNY New Paltz and is currently in the process of completing a Bachelor's in Cyber Security and Information Assurance from Western Governor's University. Al has experience working as a technical engineer for managed service providers. His responsibilities involved system and network administration, incident

response, and restoration of critical systems as needed to ensure clients maintain business continuity. He is determined to help defend against the latest threats targeting major infrastructure and institutions.

Yelisey Boguslavskiy *currently oversees AdvIntel's research and investigative and security operations. He leads AdvIntel's Security & Development Team, conducting advanced HUMINT and SIGINT investigations into cyber fraud, ransomware, APT threats, political manipulation, and violent extremist propaganda conducted through digital infrastructure. Yelisey is an author of "Security Pragmatism: The Peripheral Alliance" – a non-fiction monograph that follows 30 years of security and intelligence cooperation between Turkey, Iran, and Israel from 1947 to 1977 and beyond. Prior to Advanced Intelligence LLC, Yelisey worked as an investigator in the business intelligence community, including Kroll, a division of Duff & Phelps. He holds an M.A. degree in Security Policy Studies from the Elliott School of International Affairs of the George Washington University.*

Advanced Intelligence is an elite threat prevention firm. We provide our customers with tailored support and access to the proprietary industry-leading "Andariel" Platform to achieve unmatched visibility into botnet breaches, underground and dark web economy, and mitigate any existing or emerging threats.