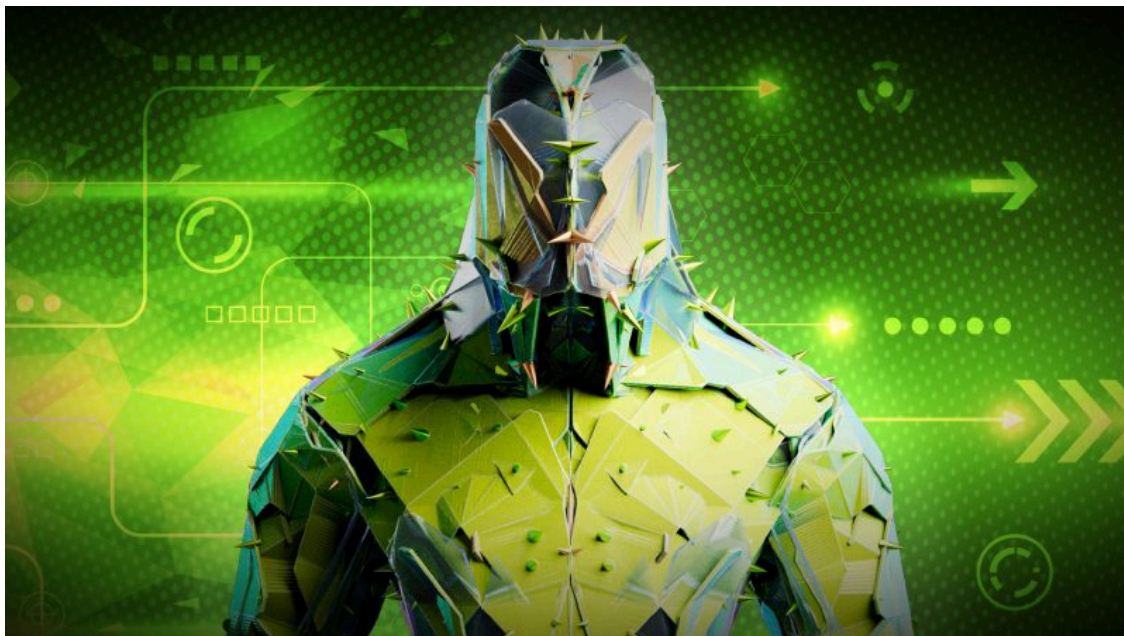


The hateful eight: Kaspersky's guide to modern ransomware groups' TTPs

By Nikita Nazarov

Published: 2022-06-23 · Archived: 2026-04-05 14:43:47 UTC

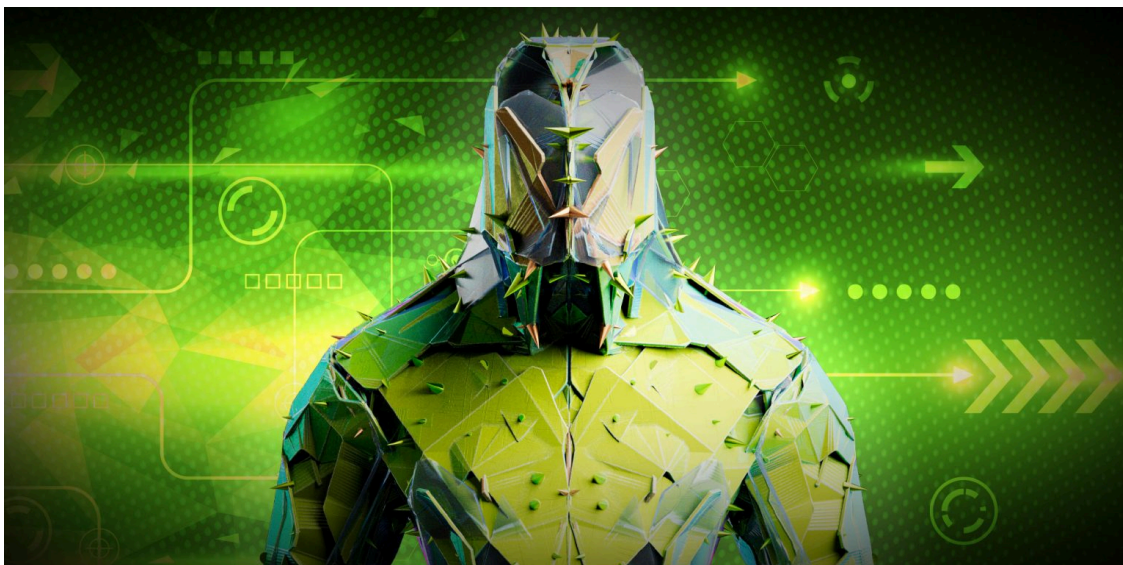


[Research](#)

[Research](#)

23 Jun 2022

2 minute read



These days ransomware analysis gets a lot of coverage in commercial and public reports, with vendors issuing dozens of ransomware-related publications each year. These reports provide analysis on specific malware families or new samples, describe the activities of a particular ransomware group, give general tips on how to prevent ransomware from working, and so on. Malware analysts and security professionals can learn a lot from these reports, but not much of the content has an immediate or practical use. With the release of the report *Common TTPs of modern ransomware*, Kaspersky experts have taken a different approach. We want to familiarize the reader with the different stages of ransomware deployment, how cybercriminals use RATs and other tools across the various stages and what they aim to achieve. The report also provides a visual guide to defending against targeted ransomware attacks, using the most prolific groups as examples, and introduces the reader to the SIGMA detection rules that we created.

What are the ransomware groups?

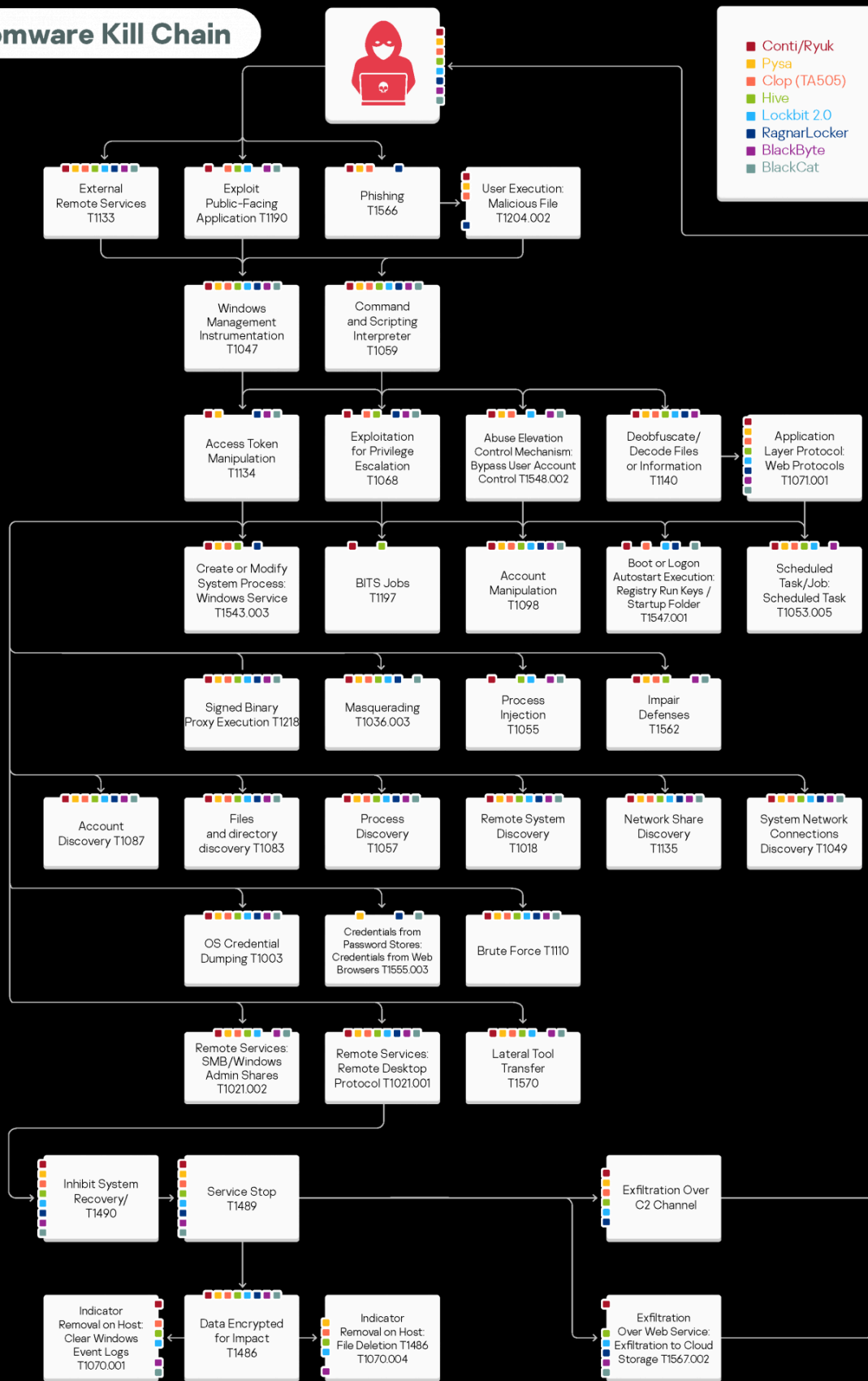
For the report we selected the eight most common ransomware groups:

1. 1 Conti/Ryuk
2. 2 Pysa
3. 3 Clop (TA505)
4. 4 Hive
5. 5 Lockbit2.0
6. 6 RagnarLocker
7. 7 BlackByte
8. 8 BlackCat

We analyzed in detail the attacks these groups perpetrated and employed techniques and tactics described in MITRE ATT&CK to identify a large number of shared TTPs. By tracking all the groups and detecting their attacks, we saw that the core techniques remain the same throughout the cyber kill chain. The attack patterns revealed are not accidental because this class of attack requires the hackers to go through certain stages, such as penetrating the corporate network or victim's computer, delivering malware, further discovery, account hijacking, deleting shadow copies, removing backups and, finally, achieving their objectives.

To highlight the common components and TTPs shared by the ransomware groups across different attack patterns, we've created a common cyber kill chain diagram. It provides a visual representation of the techniques and tactics used by different ransomware operators.

Ransomware Kill Chain



kaspersky

Once the incident data relating to the ransomware groups has been collected, we can identify the TTPs characteristic of each of them and then superimpose these onto the shared cyber kill chain. The arrows indicate the sequence of specific techniques and the colours mark the individual groups that have been known to deploy these techniques.

Whom is the report for?

This report is written for SOC analysts, threat hunting teams, cyberthreat intelligence analysts, digital forensics specialists and cybersecurity specialists that are involved in the incident response process and/or want to protect the environment they are responsible for from targeted ransomware attacks. Our main goal is to help with understanding how ransomware groups generally operate and how to defend against their attacks.

You can use this report as a book of knowledge on the main techniques used by ransomware groups, for writing hunting rules and for auditing your security solutions.

The report contains

- Tactics, techniques and procedures (TTPs) of eight modern ransomware groups: Conti/Ryuk, Pysa, Clop (TA505), Hive, Lockbit2.0, RagnarLocker, BlackByte, and BlackCat
- A description of how different groups share more than half of the common components and TTPs, with the core attack stages being executed identically across groups
- A cyber kill chain diagram that combines the visible intersections and common elements of the selected ransomware groups and makes it possible to predict the threat actors' next steps
- A detailed analysis of each technique with examples of how they are being used by various groups and a comprehensive list of mitigations
- SIGMA rules based on described TTPs that can be applied to SIEM solutions

[Download the full version of the Common TTPs of modern ransomware report \(English, PDF\)](#)



Latest Posts

Latest Webinars

Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.

Source: <https://securelist.com/modern-ransomware-groups-ttps/106824/>