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

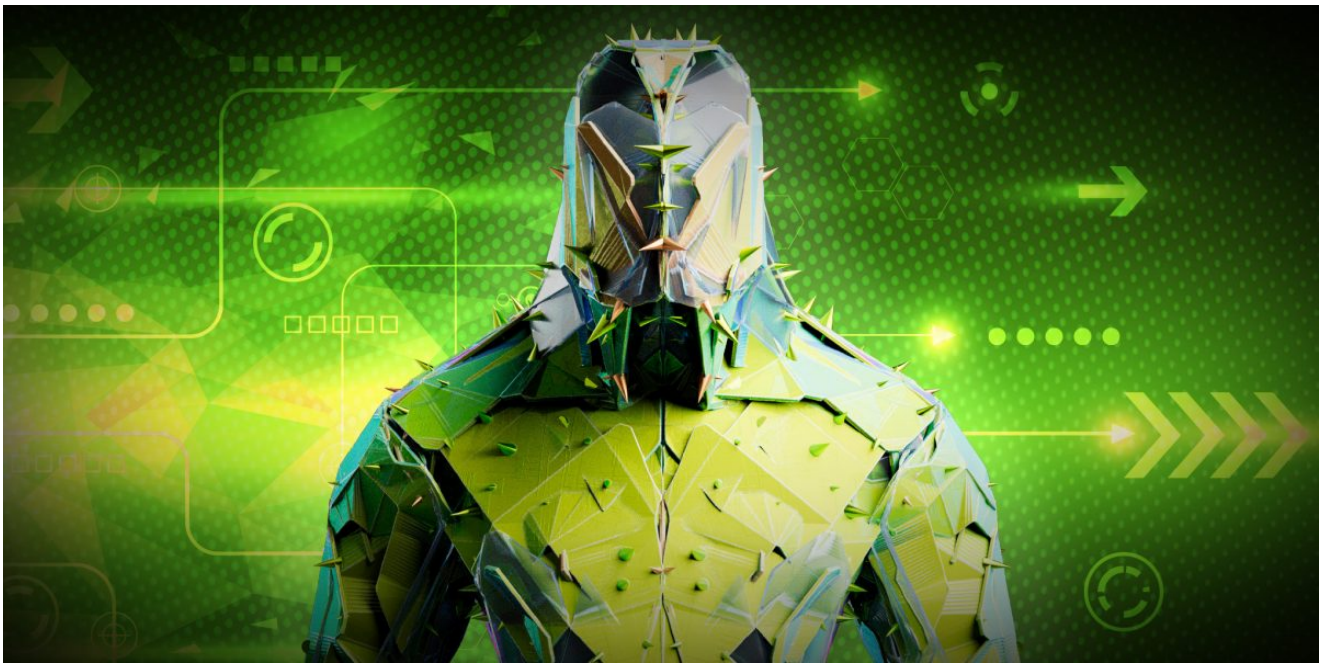
securelist.com/modern-ransomware-groups-ttps/106824/

Research

Research

23 Jun 2022

minute read



Authors

- Expert Nikita Nazarov
- Expert Vasily Davydov
- Expert Natalya Shornikova
- Expert Vladislav Burtsev
- Expert Danila Nasonov

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.

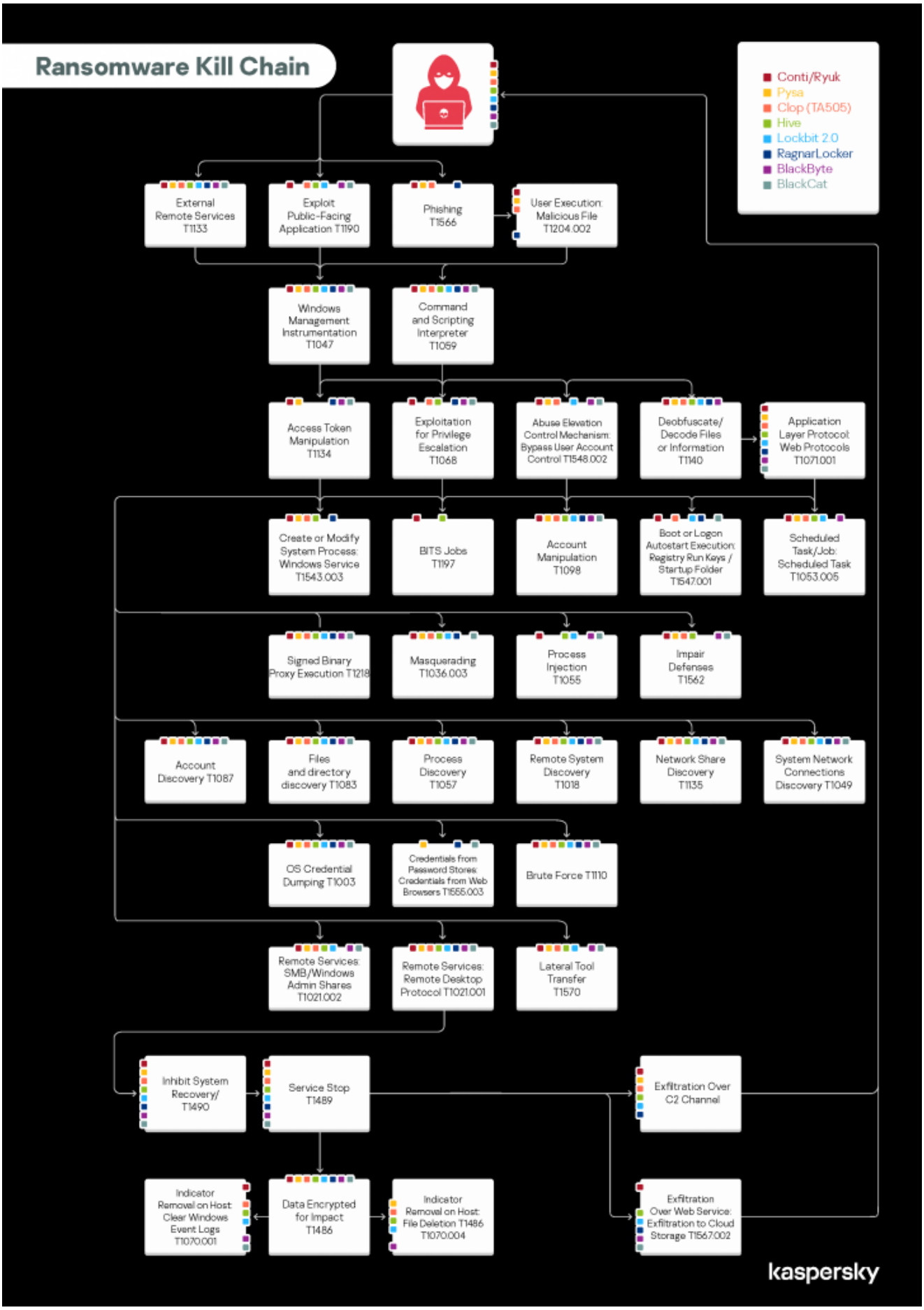
What are the ransomware groups?

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

1. Conti/Ryuk
2. Pysa
3. Clop (TA505)
4. Hive
5. Lockbit2.0
6. RagnarLocker
7. BlackByte
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
Conti/Ryuk
Pysa
Clop (TA505)
Hive
Lockbit 2.0
RagnarLocker
BlackByte
BlackCat
External Remote Services T1133
Exploit Public-Facing Application T1190
Phishing T1566
User Execution: Malicious File T1204.002
Windows Management Instrumentation T1047
Command and Scripting Interpreter T1059
Access Token Manipulation T1134
Exploitation for Privilege Escalation T1068
Abuse Elevation Control Mechanism: Bypass User Account Control T1548.002
Deobfuscate/ Decode Files or Information T1140
Application Layer Protocol: Web Protocols T1071.001
Create or Modify System Process: Windows Service T1543.003
BITS Jobs T1197
Account Manipulation T1098
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001
Scheduled Task/Job: Scheduled Task T1053.005
Signed Binary Proxy Execution T1218
Masquerading T1036.003
Process Injection T1055
Impair Defenses T1562
Account Discovery T1087
Files and directory discovery T1083
Process Discovery T1057
Remote System Discovery T1018
Network Share Discovery T1135
System Network Connections Discovery T1049
OS Credential Dumping T1003
Credentials from Password Stores: Credentials from Web Browsers T1555.003
Brute Force T1110
Remote Services: SMB/Windows Admin Shares T1021.002
Remote Services: Remote Desktop Protocol T1021.001
Lateral Tool Transfer T1570
Inhibit System Recovery/ T1490
Service Stop T1489
Exfiltration Over C2 Channel
Indicator Removal on Host: Clear Windows Event Logs T1070.001
Data Encrypted for Impact T1486
Indicator Removal on Host: File Deletion T1486 T1070.004
Exfiltration Over Web Service: Exfiltration to Cloud Storage T1567.002
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

Fill the form below to download the *Common TTPs of modern ransomware* report (English, PDF)

- Cybercrime
- Malware Technologies
- Ransomware
- Targeted attacks
- TTPs

Authors

- Expert Nikita Nazarov
- Expert Vasily Davydov
- Expert Natalya Shornikova
- Expert Vladislav Burtsev
- Expert Danila Nasonov

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

---

Your email address will not be published. Required fields are marked *

Table of Contents

GReAT webinars

13 May 2021, 1:00pm

GReAT Ideas. Balalaika Edition

---

26 Feb 2021, 12:00pm
17 Jun 2020, 1:00pm
26 Aug 2020, 2:00pm
22 Jul 2020, 2:00pm
From the same authors

How exploit packs are concealed in a Flash object

Subscribe to our weekly e-mails

The hottest research right in your inbox

-
-
-

Reports

The SessionManager IIS backdoor

In early 2022, we investigated an IIS backdoor called SessionManager. It has been used against NGOs, government, military and industrial organizations in Africa, South America, Asia, Europe, Russia and the Middle East.

APT ToddyCat

ToddyCat is a relatively new APT actor responsible for multiple sets of attacks against high-profile entities in Europe and Asia. Its main distinctive signs are two formerly unknown tools that we call ‘Samurai backdoor’ and ‘Ninja Trojan’.

WinDealer dealing on the side

We have discovered that malware dubbed WinDealer, spread by Chinese-speaking APT actor LuoYu, has an ability to perform intrusions through a man-on-the-side attack.

APT trends report Q1 2022

This is our latest summary of advanced persistent threat (APT) activity, focusing on events that we observed during Q1 2022.