Locked, Loaded, and in the Wrong Hands: Legitimate Tools Weaponized for Ransomware in 2021

X

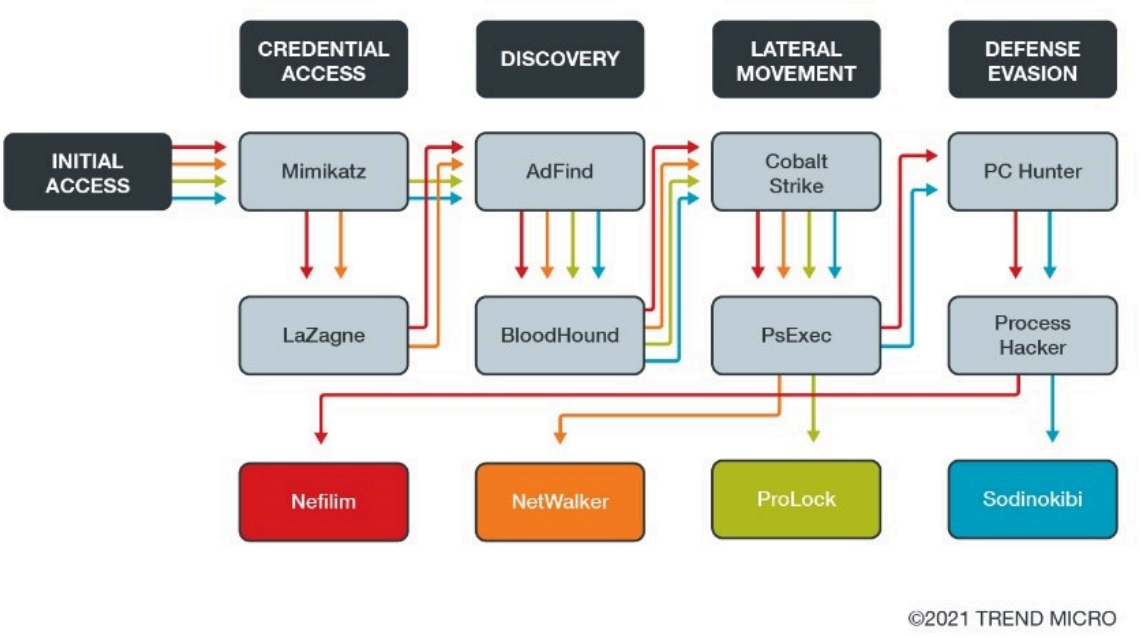
Commonly Abused Legitimate Tools

Here is a summary of some of the most commonly abused legitimate tools:

Tool	Intended Use	How It is Used for Ransomware Campaigns	Ransomware Campaigns That Used This Tool
Cobalt Strike	Threat emulation	Lateral movement, backdoor Has many other capabilities as a remote access trojan (RAT)	Clop, Conti, DoppelPaymer, Egregor, Hello (WickrMe), Nefilim, NetWalker, ProLock, RansomExx, Ryuk
PsExec	Executing processes on other systems	Arbitrary command shell execution, lateral movement	DoppelPaymer, Nefilim, NetWalker, Maze, Petya, ProLock, Ryuk, Sodinokibi
Mimikatz	Proof-of-concept code for demonstrating vulnerabilities	Credential dumping	DoppelPaymer, Nefilim, NetWalker, Maze, ProLock, RansomExx, Sodinokibi
Process Hacker	Monitoring system resources, debug software, and detect malware	Process/service discovery and termination (including antimalware solutions)	Crysis, Nefilim, Sodinokibi
AdFind	Active Directory (AD) search utility	AD discovery (can be a prerequisite for lateral movement)	Nefilim, NetWalker, ProLock, Sodinokibi
MegaSync	Cloud-based synchronization	Data exfiltration	Hades, LockBit, Nefilim

Table 1. Weaponized legitimate tools

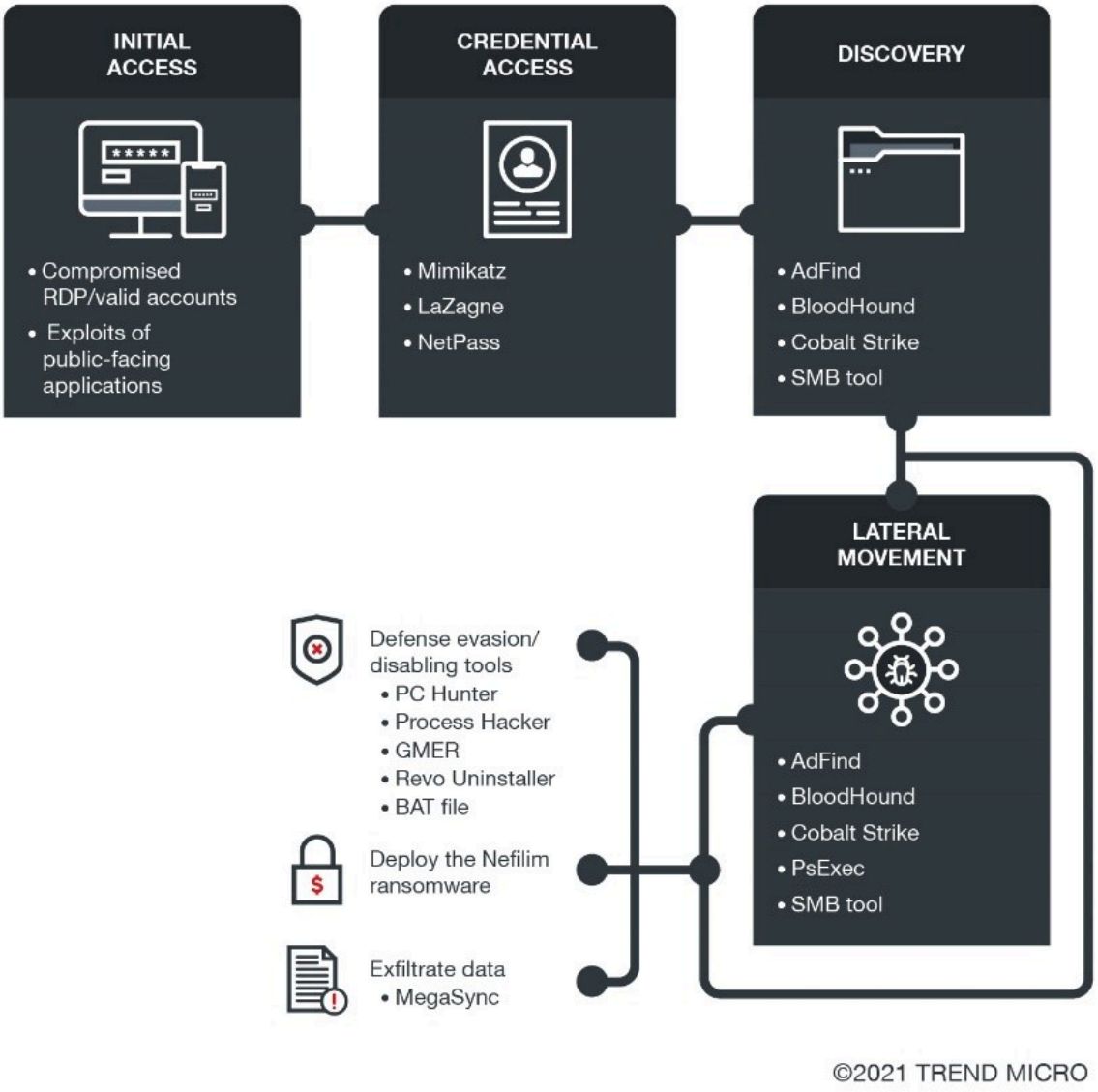
Some of the tools listed in the following figure also have similar purposes with other platforms. For example, like Process Hacker, PC Hunter, GMER, and Revo Uninstaller can be exploited to terminate antimalware solutions. Likewise, both Mimikatz and LaZagne can be used for credential dumping.



open on a new tab

Figure 1. Examples of ransomware campaigns that abuse legitimate tools for various attack stages

Notably, some campaigns use several tools at the same time, rather than just a single tool at a time, since one tool can enable the other. For example, Mimikatz, which can be abused to steal credentials, can grant access to PsExec functions that require admin privileges. One of the campaigns that employed several tools at the same time is Nefilim, which used AdFind, Cobalt Strike, Mimikatz, Process Hacker, PsExec, and MegaSync, among other tools.



open on a new tab

Figure 2. How weaponized legitimate tools are used in a ransomware campaign

In the next sections, we elaborate further on the uses of these tools as well as how they are used in ransomware campaigns.

Cobalt Strike

Tool's intended use: Cobalt Strikeopen on a new tab is meant to be used as a threat emulation software that can perform reconnaissance, covert communication, spear phishing, and post-exploitation. It is used by security researchers for a variety of functions, including penetration testing.

Possible uses for ransomware: Cybercriminals use this tool in campaigns for lateral movementopen on a new tab or as a backdoor. As a RAT, it also has many other capabilities. This tool can avoid detection by obfuscating shellcode and using Malleable Command and Control (aka Malleable C2).

Campaigns that it was used for: Some ransomware campaigns that abused Cobalt Strike are Conti, Clopopen on a new tab, DoppelPaymer, Egregoropen on a new tab, Helloopen on a new tab (WickrMe), NetWalkeropen on a new tab, Nefilimnews- cybercrime-and-digital-threats, ProLockopen on a new tab, RansomExx, and Ryuk, and Sodinokibiopen on a new tab. We also found that it is compatible with proof-of-concept ransomware Povlsomware.

In our recent analysis on Conti, the ransomware dubbed as the successor of Ryuk, we discussed how Cobalt Strike beaconsopen on a new tab (Cobalt Strike's covert payload) served as backdoors for the attack. The tool was also used for lateral movement. This was performed via actions such as accessing and dumping credential hashes from LSASS, using the harvested passwords for further movement, sending files to remote drives, and using Windows Management Instrumentation (WMI) commands to run either a DLL or EXE copy of itself.

PsExec

Tool's intended use: PsExecopen on a new tab is a "light-weight telnet-replacement" utility that lets users run Windows Server processes on remote systems. It also features full interactivity for console applications without needing to install the client software manually.

Possible uses for ransomware: With attackers leveraging the features that enable a user to execute processes on remote systems, PsExec can be abused for arbitrary command shell execution and lateral movement. PsExec can also be used for propagation and remote execution of ransomware.

Mimikatz

Tool's intended use: Mimikatzopen on a new tab is intended to be, in the tool creator's own words, "A little tool to play with Windows security." Mimikatz was built as a proof-of-conceptopen on a new tab code to demonstrate the vulnerabilities in Microsoft authentication protocols. It can harvest passwords, hashes, PIN codes, and Kerberos tickets.

Possible uses for ransomware: Cybercriminals employ the features of Mimikatz for credential dumpingopen on a new tab to extract usernames, passwords, and other credentials that might be used to escalate privilege in other phases of the attack.

Campaigns that it was used for: Attacks where Mimikatz is abused include those for DoppelPaymer, Nefilim, NetWalker, Mazeopen on a new tab, ProLockopen on a new tab, RansomExx, and Sodinokibiopen on a new tab.

NetWalker can be executed filelessly using legitimate programs in the system; the ransomware is not compiled but is written in PowerShell and executed in the memory directly without needing to store the actual binary into the disk. The sample from the campaign that we observed abused PowerSploit's Invoke-Mimikatz, an open-source program that can reflectively load Mimikatz. After being loaded, the tool can then perform credential dumping. Other campaignsopen on a new tab have also shown how NetWalker launches Mimikatz to steal credentials that will then be used to launch PsExec and deploy the said ransomware.

Similar tool: LaZagneopen on a new tab, an open-source application used to retrieve passwords for various software, has also been exploited for credential dumping in campaigns for several ransomware variants such as RansomExx and Nefilim and NetWalkeropen on a new tab. NetPass can also be used to gather credentials.

Process Hacker

Tool's intended use: Process Hackeropen on a new tab is a free tool that is intended to be used to identify and stop processes. In turn, it can be employed for detecting malware, monitoring system resources, and debugging software. It can pinpoint runaway processes, processes that are using a particular file, programs that have active network connections, and real-time information on disk access and usage, among other things.

Possible uses for ransomware: As Process Hacker can be used to gain an overview of processes currently being used, cybercriminals have weaponized this function for ransomware campaigns to discover and terminate arbitrary processes and services, including those that are antimalware-related.

Campaigns that it was used for: Campaigns that benefited from this tool include Crysisopen on a new tab, Nefilim, and Sodinokibi. The tool was used to identify and disable antimalware solutions.

Crysis (aka Dharma) has, on several occasions, used Process Hacker to alter processes and security solutions. The installer of the tool was also part of a 2018 attackopen on a new tab as prc.exe. A more recent attackopen on a new tab also used the tool (as Processhacker.exe) for similar functions.

Similar tools: Tools such as PC Hunteropen on a new tab (which grants access to system processes, kernel modes, and hooks), GMERopen on a new tab (which detects and removes rootkits) and Revo Uninstalleropen on a new tab (which can uninstall apps and programs) also terminate programs and antimalware solutions. Similar to the case of Process Hacker, the three have been used in Crysis and Nefilim campaigns.

AdFind

Tool's intended use: AdFindopen on a new tab is a free command-line AD query tool that can be used to collect information from AD. AdFind can query AD for computers, identify domain users and domain groups, extract subnet information from AD, and collect information about organizational units on domain trusts.

Possible uses for ransomware: AdFind can be used to discover computers, users, or groups with AD as a reconnaissance tool, as well as to equip ransomware with the resources that it needs for lateral movement via AD.

MegaSync

Tool's intended use: MegaSyncopen on a new tab is a cloud-based synchronization tool that is designed to work with the MEGAopen on a new tab file-sharing service. It lets users sync files to devices and can also be used for storing and managing files, as well as for collaborating and sharing data with other users.

Possible uses for ransomware: MEGA and MegaSync can be used for data exfiltration — a vital step for recent ransomware campaigns that wield the double extortion technique, since they not only encrypt files but also steal and threaten to publicly expose a targeted company's sensitive data.

Campaigns that it was used for: Hadesopen on a new tab, LockBitopen on a new tab, and Nefilimnews-cybercrime-and-digital-threats are some of the ransomware campaigns that used this tool.

LockBit is one of the ransomware variants that employs the double extortion technique. The LockBit ransomware operators employ MegaSync for exfiltration, taking advantage of the storage and ease of access of the tool to be

able to quickly upload files from the affected system.

Defense Against Disguised Enemies

The presence of weaponized legitimate tools must be detected so that security teams can stop a ransomware campaign dead in its tracks. However, this is easier said than done as these tools might evade detection in several ways. One is through features that can be used to implement evasion techniques, like in the case of Cobalt Strikeopen on a new tab. Cybercriminals can also alter the codeopen on a new tab of these tools to tweak parts that trigger antimalware solutions.

Additionally, when spotted from a single entry point (for example, when looking at the endpoint alone), the detections might seem benign by themselves, even when they should raise the alarm — that is, if they were viewed from a broader perspective and with greater context with regard to other layers such as emails, servers, and cloud workloads.

In tracking ransomware campaigns, organizations would be better protected if they rely not only on detections of files and hashes but also on monitoring behavior across layers. This is what we did for our recent investigation on the Conti ransomwarenews article, which we tracked using Trend Micro Vision One™ products.

Solutions such as Trend Micro Vision One provide increased visibility and correlated detections across layers (endpoints, emails, servers, and cloud workloads), ensuring that no significant incidents go unnoticed. This allows faster response to threats before they can do any real damage to the system.

Indicators of Compromise (IOCs)

Note: Actual detections might vary based on the hashes involved in the attack.

Tool	Trend Micro Pattern Detection
Cobalt Strike	Backdoor.Win64.COBEACON.SMA
PsExec	N/A Recommendation: Check suspicious PsExec activity in SMB network and shared folders
Mimikatz	HackTool.Win32.MIMIKATZ.SMGD
Process Hacker	PUA.Win64.ProcHack.AC
PC Hunter	PUA.Win64.PCHunter.A
GMER	PUA.Win32.GMER.A
LaZagne	HackTool.Win64.LAZAGNE.AE

HIDE

Like it? Add this infographic to your site:

1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Cracking the Isolation: Novel Docker Desktop VM Escape Techniques Under WSL2news article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article
- The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---