WatchTower | Trends and Top Cybersecurity Takeaways from 2022

January 26, 2023
by SentinelOne

Gathering information about cyber attacks is only half of the battle – the other half lies in curating the raw data into original insights about major vulnerabilities, cybercrime toolkits, and ransomware groups.

In this blog post, SentinelOne's WatchTower team reflects on a year's worth of threats observed and investigated across every geography and industry our partners operate in. Based on telemetry from tens of millions of endpoints protected by Singularity XDR platform, here's a review of the top cyber attack trends from 2022 and their significance in the fluctuating threat landscape.

Trends In the Landscape | 2022 Top Cybersecurity Takeaways

Findings from 2022 show the top ransomware variants, initial infection vectors, and emerging malware that organizations from all sectors contended with.

Ransomware Findings

Over the course of last year, ransomware showed no signs of slowing down. Faced with federal level sanctions, the act of rebranding is now a widespread strategy ransomware groups use to obfuscate their identities and sidestep crackdowns. Several new ransomware groups emerged in 2022 and existing ones rebranded before showing their faces in the threat landscape once more.

- Quantum ransomware operation became Dagon Locker
- Notorious cybergang Conti siphoned their brand into smaller groups including Hive, BlackCat, and HelloKitty
- DarkSide transitioned into BlackMatter, followed by further splinters including AlphV.
- DoppelPaymer rebranded into Grief
- Rook ransomware transitioned into Pandora

Ransomware authors have also widely adopted both Rust and Golang in their efforts to evade detection. BlackCat, Hive, and a host of other ransomware families also made the switch, taking advantage of their fast file encryption capabilities and wide-ranging cryptographic libraries.

Growing Infection Vectors

2022 saw a steep increase in supply chain attacks, SEO poisoning/malvertising, and cracked software. The growing theme in attacks from last year saw threat actors steering towards the path of least resistance for greater rewards.

Through software supply chain attacks, actors exploit weaknesses in a vendor's development cycle to inject malicious code into a certified application. While many organizations have worked to monitor and detect such threats since the attack on SolarWinds in 2020, threat actors are still leveraging open-source modules for initial intrusion. Identity management giant, Okta for example, found themselves the target of a supply chain attack last year when its 2FA provider, Twilio, was breached.

SEO poisoning has also risen to the top as a way for threat actors to take advantage of existing infrastructure for malicious purposes. By poisoning the mechanisms that influence search engine optimization (SEO), attackers have been able to quickly lure and infect unsuspecting users with commodity malware. Cracked software follows the same theme, banking on victims to download unlocked, illegal software which is embedded with dangerous malware.

Malware Innovations

Attackers were observed attempting to neutralize and sidestep endpoint detection and response (EDR) tools over the past year, using bypass techniques and known vulnerabilities. In February 2022, the FBI and United States Secret Service (USSS) released a joint cybersecurity advisory warning against BlackByte; a ransomware group known for using a "Bring Your Own Driver" technique to circumvent various EDR products available on the market today.

A table of ransomware groups that created modules attempting to kill EDR solutions in 2022 is provided below. SentinelOne offers robust anti-tamper capabilities to protect against these attacks.

Ransomware Group	Affiliated Driver Files Targeting EDR Solutions
RobinHood	RBNL.SYS, gdrv.sys
CUBA, AvosLocker	aswArPot.sys
(Genshin Impact) > Rever	mhyprot2.sys
BlackByte Ransomware	RTCore64.sys and RTCore32.sys
Lockbit	Apchelper.sys, 2.sys, hrwfpdrv.sys
Hive	Pertry.sys, Deame.sys
BlackBasta	procexp.Sys
Lapsus$	Mrjowv.sys

The threat intelligence community observed new wiper malware samples and ransomware strains circulating in Ukrainian organizations. The malware was distributed with the goal of rendering their computer systems inoperable. HermeticWiper and PartyTicket ransomware were among the novel threats prefacing the unprovoked Russian invasion of Ukraine that have since evolved to produce several new malware variants. SolarMarker infostealer, Bumblebee downloader, and the Raspberry Robin worm (*aka* QNAP worm, or LNK worm) also emerged as popular tools for cyber attackers in 2022.

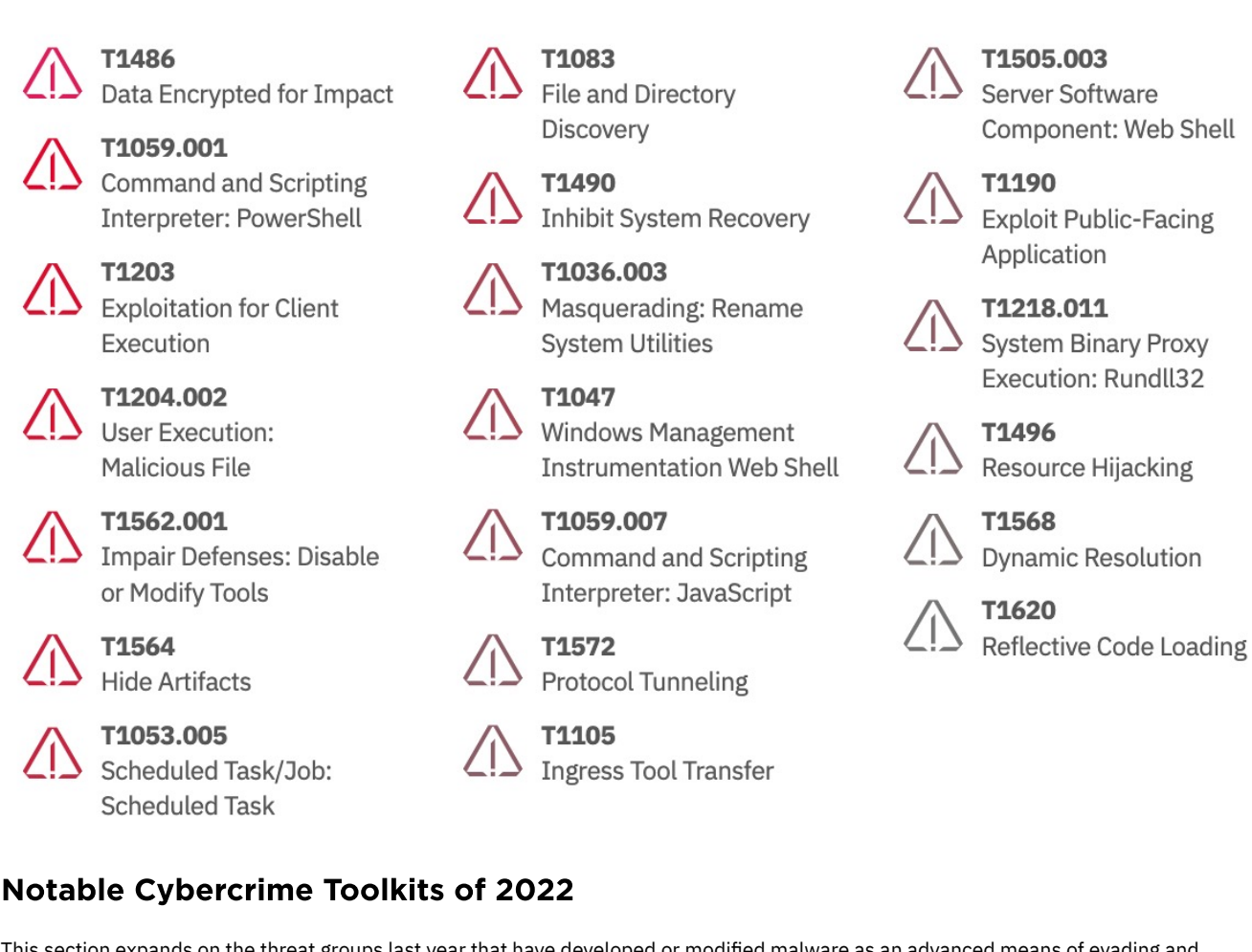
2022 Most Used Commodity Tooling & Techniques

Attackers will always look for opportunities to do less work for more damage. They don't always use sophisticated and customized malware and often rely on the same public tools used by network administrators and security professionals.

The most notable commodity tooling observed in 2022 by threat tactic are as follows:

- Reconnaissance – Ipconfig, Net.exe, Netstat, Nslookup, arp.exe, WMI, Impacket, Cobalt Strike, Whoami, ADFind, ADRecon.py, Advanced Port Scanner, IP Scanner, PingCastle, Powerview, and Winrm
- Credential Theft – Mimikatz, Meterpreter, Cobalt Strike, BloodHound, SharpHound, ProcDump, Process Hacker, ninjacopy, NirSoft, Lazagne, and PassView
- Lateral Movement – Psexec, PDQ Install, Winrm, SMB, WMI, RDP, SSH
- Remote Access – TeamViewer, AnyDesk, Splashtop, ZohoAssist, ConnectWise, VNC, BeyondTrust, GoToAssist, RemotePC, TightVNC, RDP(mstsc), Registry terminal server enable
- Defense Evasion – Gmer, Icesword, Regedit (reg.exe), Process Hacker driver, Powershell, WMI, Service Kill (bat file), Process Kill (bat file)
- Staging – SCCM, Group Policy, Psexec, Powershell Remote, ConnectWise
- Data Exfiltration – RClone, FileZilla, Winscp, cloud services such as MegaSync and megacloud)

The most commonly observed MITRE ATT&CK techniques over the last 12 months were:



Notable Cybercrime Toolkits of 2022

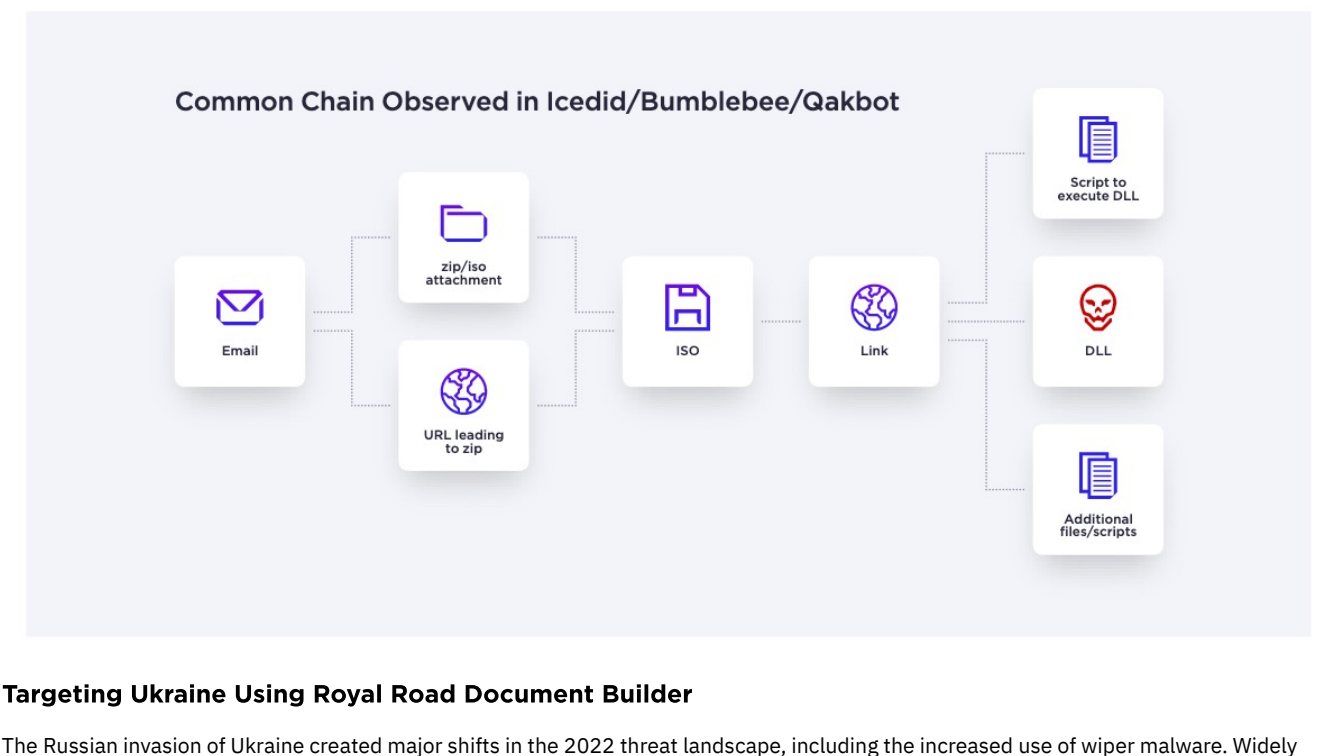
This section expands on the threat groups last year that have developed or modified malware as an advanced means of evading and disabling detection and response mechanisms.

Black Basta Ransomware & Ties to FIN7

Ransomware-as-a-Service (RaaS) group, Black Basta, is well known for launching double extortion attacks through customized tools. During analysis of their toolkit, SentinelLabs researchers found that the group had worked with a developer associated with Carbanak/FIN7 – a threat gang specializing in targeting U.S. retail and hospitality sectors. Uncovering possible connections between threat groups lends cybersecurity analysts better visibility into a wider net of threat operators' infrastructures.

Transformers | Bumblebee Downloader, IcedID and Qakbot

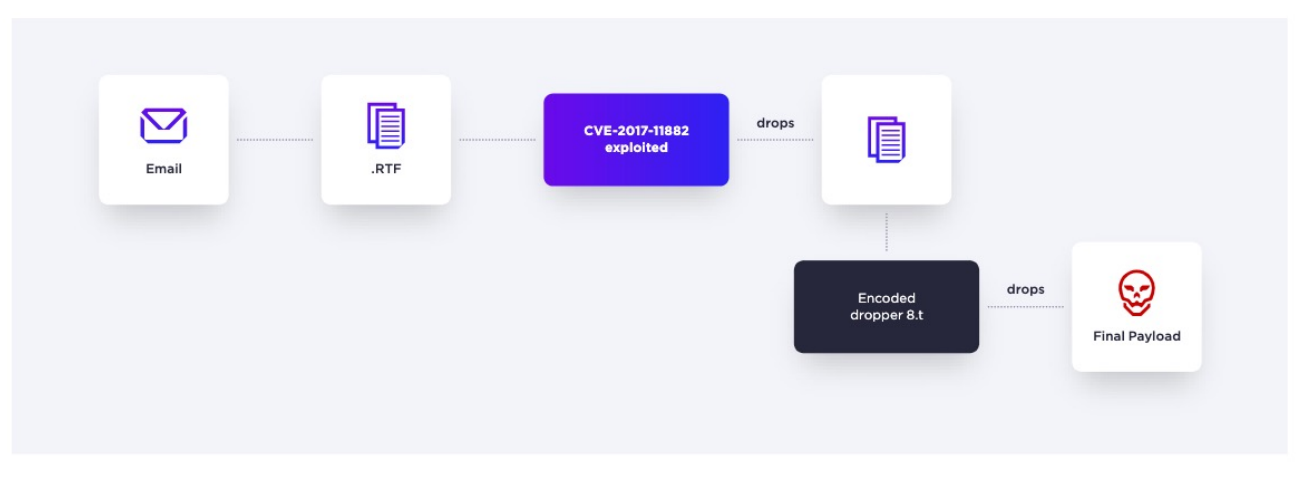
First identified in March 2022, the Bumblebee downloader has been adopted by multiple threat groups as a sophisticated initial access facilitator. Bumblebee allows threat actors to gain initial access to enterprise environments and launch advanced cyberattacks. This downloader also shares the same infection chain as Qakbot; another toolkit that appeared multiple times in the past year along with IcedID malware.



Targeting Ukraine Using Royal Road Document Builder

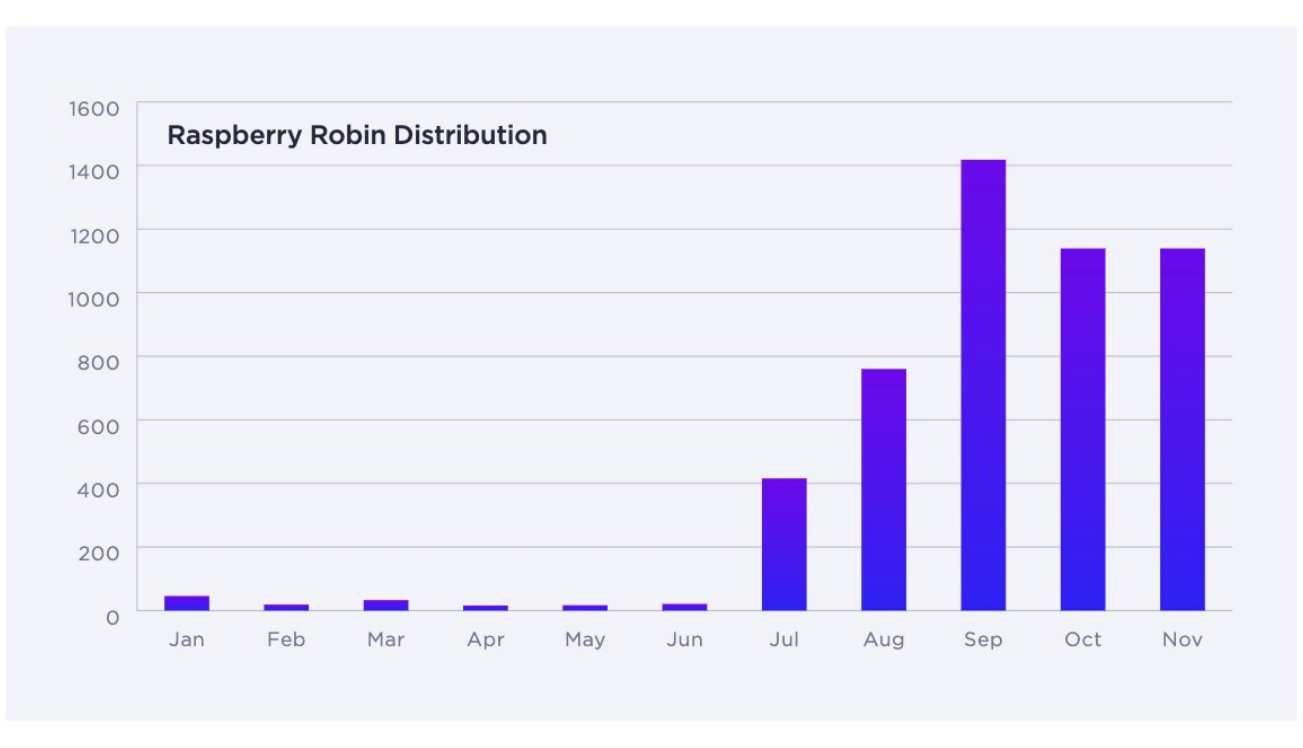
The Russian invasion of Ukraine created major shifts in the 2022 threat landscape, including the increased use of wiper malware. Widely impacting Ukrainian citizens as well as organizations based outside of Ukraine was the Royal Road Document Builder.

SentinelLabs' analysis indicates that the threat actors behind these cyberattacks are part of a Chinese state-sponsored cyber espionage group which uses phishing emails to deliver these malicious documents and exploit the Bisonal backdoor.



Raspberry Robin Worms Its Way Through 2022

Last year, threat actors accelerated their use of Raspberry Robin to deliver multiple types of malware and ransomware to infected endpoints. Also known as the QNAP or LNK worm, Raspberry Robin is a self-propagating worm used in attacks as a delivery mechanism for second stage malware. Its usage amongst threat actors spiked in the latter half of 2022 making it the fastest growing threat families of last year.



SocGholish Expands and Diversifies

Highly active throughout the past 12 months, SocGholish has undergone a marked diversification, expanding infrastructure to contend with known defenses. Across 2022, SocGholish averaged 18 malware-staging servers being unveiled each month. Threat groups use a JavaScript-based framework to gain initial access to targeted systems in campaigns that primarily revolve around social engineering tactics. SocGholish has been able to persist in the threat landscape, which emphasizes the need for enterprises to regularly audit the integrity of their web servers, websites, and DNS records.

DLL Sideloading Attacks Continue to Menace

Major threat groups or malware families including Qakbot, Sliver Framework, Temp.Hex, FIN7, and LockBit led the uptick in sideloading DLL files to execute malicious payloads in attacks from 2022. This tactic allows cyber criminals to sidestep first-generation EDR solutions and legacy antivirus products while installing malware on targeted devices.

Conclusion

2022 showed that threat actors continue to use what works while investing in novel techniques in response to countermeasures by security teams and security software.

Identifying and sharing trends in new vulnerabilities, attack vectors, and malware strains are key to staying steps ahead of cyber attackers. Though new threats will undoubtedly continue to emerge, there are many ways enterprises can mitigate risk and harden their defenses. The more information that is shared about past, current, and emerging threat actors, the better enterprises can implement the people, processes, and technology needed to combat cybersecurity challenges.

Looking ahead to 2023, threat actors will continue to upgrade their methods and tools of attack, innovating on attack vectors and finding new vulnerabilities. Establishing an effective response strategy and deep, continuous monitoring can help augment a business' in-house team's defenses with robust detection and response capabilities.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- The Advantages of eBPF for CWPP Applications
- SentinelOne's Cybersecurity Predictions 2023 | What's Next?
- Apple's macOS Ventura | 7 New Security Changes to Be Aware Of
- Decoding the 4th Round of MITRE ATT&CK® Framework (Engenuity): Wizard Spider and Sandworm Enterprise Evaluations
- Bringing Identity to the Era of XDR
- Best-of-Breed Identity Threat Detection and Response Meets Best-of-Breed XDR