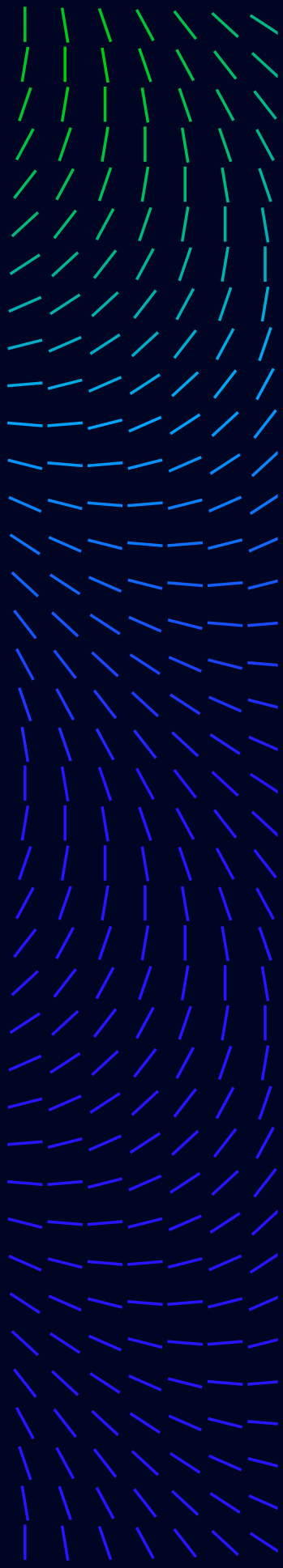
Trellix

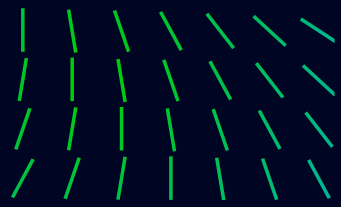
TRELLIX THREAT LABS RESEARCH REPORT

APRIL 2022

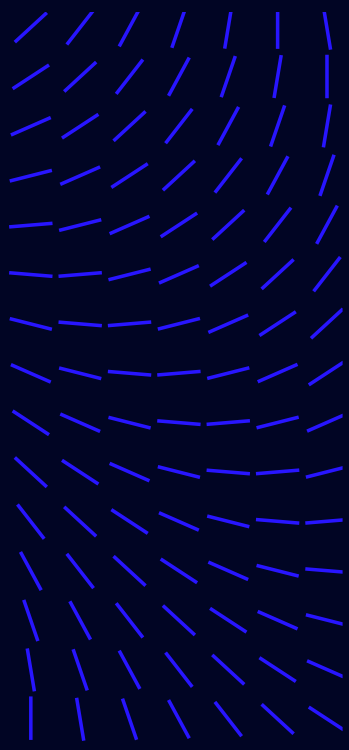
REPORT

TABLE OF CONTENTS





The fourth quarter of 2021 saw the world shift out of a two-year pandemic during which bad actors leveraged work from anywhere opportunities and Log4Shell was an unwanted holiday guest. During the first quarter of 2022, the focus on threats shifted to campaigns weaponizing cyberthreats against Ukrainian infrastructure in the Eurasia region conflict. Our latest Trellix Threat Labs Research Report includes our findings from Q4 2021, our identification of a multi-stage espionage attack on high-ranking government officials, and our recent analysis of cyberattacks targeting Ukraine and the newly identified HermeticWiper during Q1.

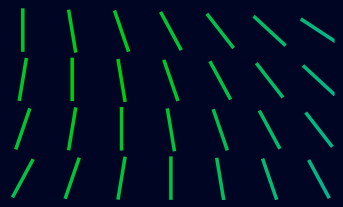


LETTER FROM OUR LEAD SCIENTIST

Welcome to our latest threat report.

Nearly a quarter into the new year, it would be an understatement to say that we had an easy start of the year. We are slowly moving out of the pandemic, but uncertainty around the recent conflicts in the Eurasia region dominates our daily lives and conversations.

First, Trellix stands for peace. No matter which parties are involved in any conflict, our mission is to protect our customers and comply with international laws. Our research and vigilance continued as we prepared this report. For example, the Lapsus$ group attacked major corporations around the world with an initial focus on South American victims, leaking sensitive data including source-code and certificates.



We observed those certificates being abused. An example to sign malware binaries, a method to attempt bypassing the trust of operating systems and security products. Details of this group, their latest breach and countermeasures can be read here.

In our second threat report since the launch of our new company, we acknowledge the (cyber) events that dominated global headlines. From attacks on Ukrainian infrastructure to HermeticWiper malware destroying the boot sectors of any infected machine, cybersecurity was top of mind for many in the new year. We also look back at the fourth quarter of 2021, which saw the Log4shell vulnerability impact hundreds of millions of devices and many now brace for new threats coming in the new year.

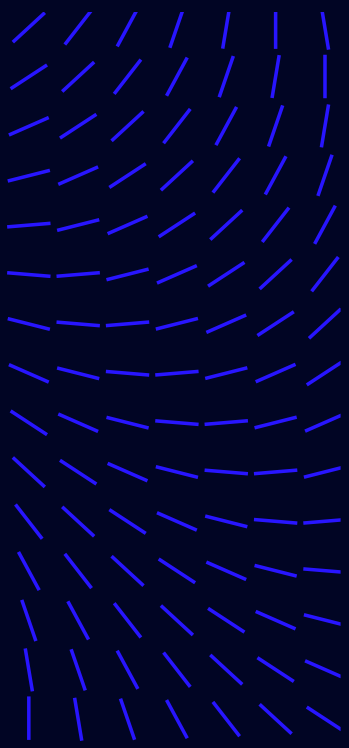
The Trellix Threat Labs team has been at the frontline of analyzing and researching ransomware for many years. Working together with the public sector, we were proud to celebrate success when in December 2021 arrests were made and ransomware operations were shut down. The recent leaks of chats from both the Conti ransomware group and the Trickbot malware group revealed how professional these operations are run. It demonstrates that we need a united answer between public and private sectors to stop the disruption of these attacks.

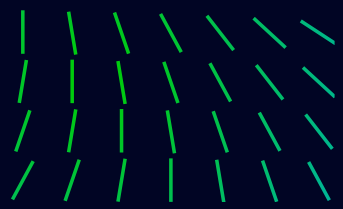
In addition, please check out our **Trellix Threat Labs blog page** featuring our latest threat content, videos, and links to the security bulletin.

This report also spotlights other prevalent threats and attacks observed in the wild.

— *Christiaan Beek*
Lead Scientist

Twitter @ChristiaanBeek





TRELLIX THREAT LABS ANALYSIS OF CYBERATTACKS TARGETING UKRAINE, PLUS HERMETICWIPER

Analysis from the Trellix Labs Threat team into the activity of wipers being deployed within the Ukraine leads them to believe that there is likely is a connection between Whispergate and the newly identified HermeticWiper.

See more of our intelligence and analysis of threat activity in the Ukrainian region.

RECOMMENDED STEPS TO PREVENT INITIAL ACCESS

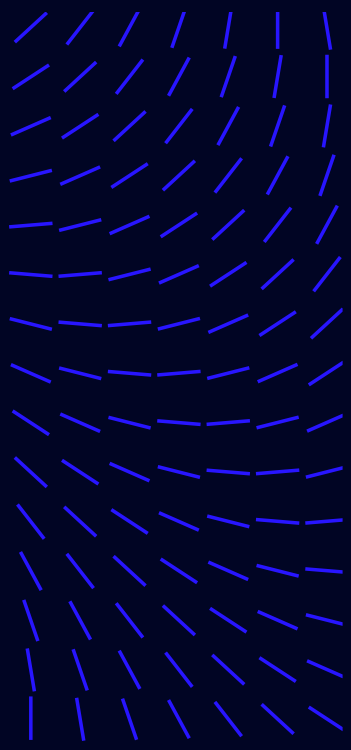
Organizations should look to review the Initial Access Tactics, techniques, and procedures (TTPs) associated with Russian nation state activity to proactively protect their environment from infiltration.

- Phishing/Spearphishing attacks utilizing shortened URLs of malicious domains.
- Monitor for brute force activity to identify valid account credentials and Microsoft 365 Accounts.
- Enable multifactor authentication (MFA) for all users, without exception.
- Exploiting Public Facing Systems – CISA maintains a full list of CVEs that are known to be exploited.
- Disabling all ports and protocols that are not essential, especially anything related to remote services.
- Hunt and block open-source tools not related to business activities that have been seen in prior attacks – UltraVNC, AdvancedRun, wget, and impacket.

Other threat campaigns and groups targeting Ukraine include:

ACTINIUM APT	IsaacWiper
Agent Tesla	NOBELIUM APT
CaddyWiper	OutSteel
CERT-AU 4109	RURansom Wiper
DDoS Attacks	SaintBot
Gamaredon APT	Shuckworm APT
Gamaredon APT	UAC-0056

Go to our Trellix Threat Center to preview and stay ahead of emerging threats, including HermeticWiper.



TRELLIX LABS DISCOVER SUSPECTED DARKHOTEL APT ACTIVITY UPDATE

In March our team discovered a first-stage malicious campaign targeting luxury hotels in Macao, China since the latter half November 2021. The attack started with a spearphishing email directed to the hotel's management staff in roles like the vice president of HR, assistant manager, and front office manager. Based on the job titles we can assume that the targeted individuals have sufficient access into the hotel's network, including the book systems. How it works:

- The email used for this spear-phishing attack contains an attachment with an Excel sheet. The Excel sheet is used to trick the victim and enable malicious macros embedded when it's opened.
- Those macros enable several mechanisms detailed in the Technical Analysis part and summarized in the Infection Flow Chart below.
- In the beginning, macros create a schedule task to perform recognition, data listing, and data exfiltration.
- Then, to enable communication with the Command-and-Control server used to exfiltrate victim data, macros are using a know lolbas (Living Off the Land Binaries and Scripts) technique to perform PowerShell command lines as trusted script.

Read our blog for more DarkHotel APT background, attribution, campaign, and technical analysis.

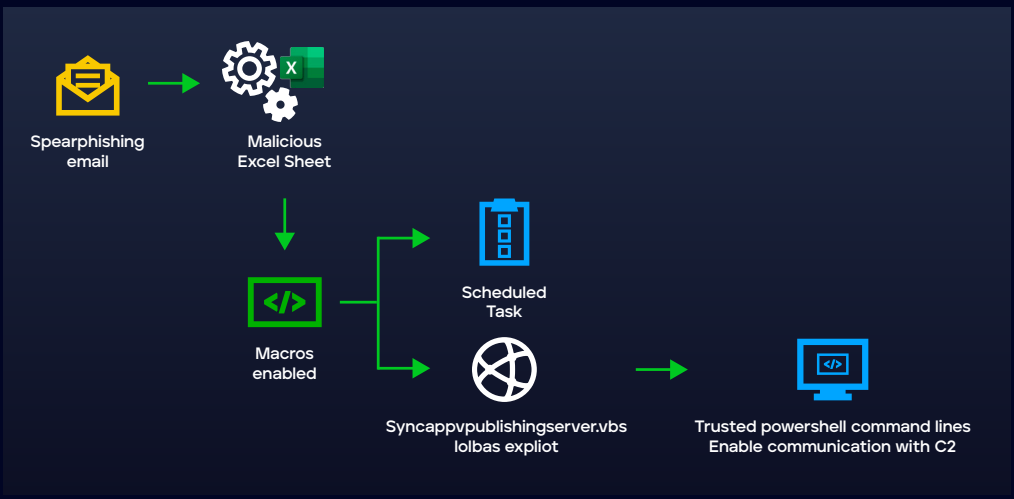


Figure 1. Execution flow of the attack

TRELLIX THREAT LABS IDENTIFY PRIME MINISTER'S OFFICE COMPROMISE

In January our team announced its identification of a multi-stage espionage campaign targeting high-ranking government officials overseeing national security policy and individuals in the defense industry in Western Asia. Trellix undertook pre-release disclosure to the victims and provided all necessary content required to remove all known attack components from their environments.

Analysis of the attack process begins with the execution of an Excel file containing an exploit for the MSHTML remote code execution vulnerability (CVE-2021-40444). This is used to execute a malicious DLL file acting as a downloader for the third stage malware we called Graphite. Graphite is a newly discovered malware sample based on a One-Drive Empire Stager which leverages OneDrive accounts as a command and control server via the Microsoft Graph API.

The last phases of this multi-stage attack, which we believe is associated with an APT operation, includes the execution of different Empire stagers to finally download an Empire agent on victims' computers and engage the command and control server to remotely control the systems.

The following diagram shows the overall process of this attack.

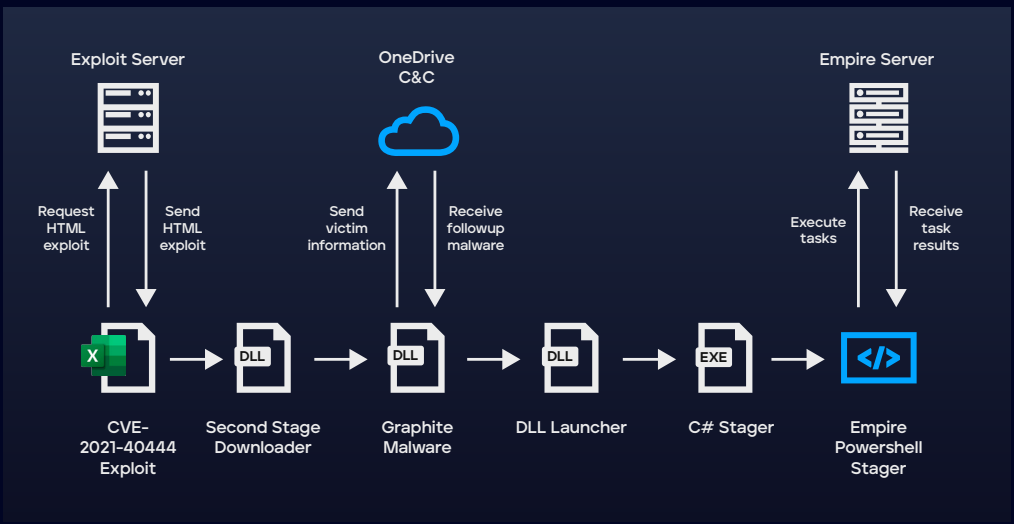
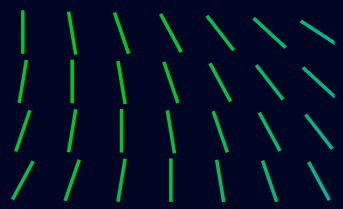


Figure 2. Attack flow

Read our blog for more in-depth analysis including stages, infrastructure, and attribution.



METHODOLOGY

Trellix's backend systems are providing telemetry that we use as input for our quarterly threat reports. We combine our telemetry with open-source intelligence around threats and our own investigations into prevalent threats like ransomware, nation-state activity, etc.

When we talk about telemetry, we talk about detections, not infections. A detection is when a file, URL, IP-address, or other indicator is detected by one of our products and reported back to us.

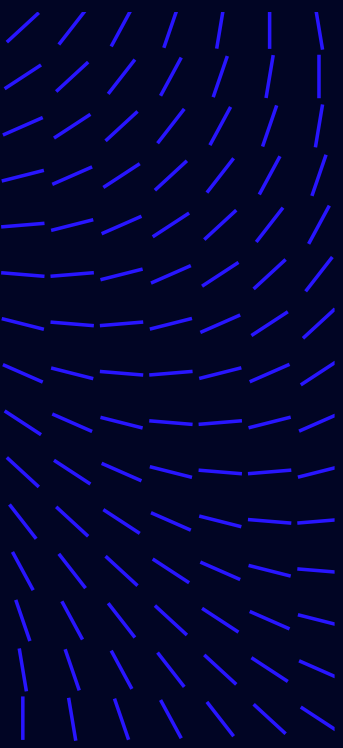
Privacy of our customers is key. It also is important when it comes down to telemetry and mapping out to sectors and countries of our customers. Client-base per country differs and numbers could be showcasing increases while we have to look deeper into the data to explain. An example is that the Telecom sector is always scoring high in our data. It doesn't mean necessarily that this sector is highly targeted. The Telecom sector contains ISP providers as well that own IP-address spaces that can be bought by companies. What does that mean? Submissions from the ip-address space of the ISP are showing up as Telecom detections, but could be from ISP clients that are in a different sector operating.

RANSOMWARE

In the final quarter of 2021, the ransomware landscape continued to change. In lieu of the large attacks we described in our previous report, ransomware actors had to find a new underground home and law enforcement started to crack down on several high-profile ransomware groups. One of these groups was REvil/Sodinokibi, which was still ranked amongst the top ransomware families in Q3. However REvil left the stage after a coordinated takedown of their infrastructure, several internal disputes and members being arrested. Trellix is proud to have assisted in the REvil investigation by providing malware analysis, locating key infrastructure, and identifying multiple suspects.

Our top 3 in Q4 2021 belonged to Lockbit, Cuba, and Conti ransomware. We suspect that remaining members of REvil most likely have found a new home with these ransomware families.

While the ink for this report is barely dry, the landscape has shifted yet again. Conti, which has grown to one of the largest families, had thousands of internal chats leaked on the internet, essentially exposing their inner secrets. We dubbed this leak the Panama Papers of Ransomware and we will be sure to highlight our findings in the next quarterly report.



To help enterprises better understand and defend against ransomware attacks in the threatscape, our Threat Labs team presents research and findings into the prevalence of a wide variety of ransomware threats, including families, techniques, countries, sectors, and vectors from Q4 of 2021.

289%

increase in Media and Communications category from Q3 to Q4 of 2021.

▼61%

Ransomware detections among United States-based clients decreased from Q3 to Q4 of 2021.

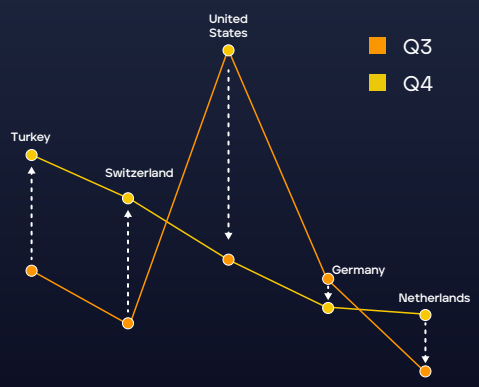
RANSOMWARE CUSTOMER SECTORS

- Business Services
- Non-Profit
- Government
- Media and Communications
- Transportation and Shipping

MOST REPORTED RANSOMWARE MITRE ATT&CK TECHNIQUES

1. Data Encrypted for Impact
2. File and Directory Discovery
3. Obfuscated Files or Information
4. Process Discovery
5. Process Injection

CHANGE IN RANSOMWARE CLIENT COUNTRIES



RANSOMWARE FAMILY DETECTIONS

	Lockbit	Cuba	Conti	Ryuk	BlackMatter
Q3	4%	8%	6.7%	7%	N/A
Q4	23%	19%	17%	11%	7%

NATION-STATE ACTIVITY

Our team tracks and monitors Nation-State campaigns and associated indicators and techniques. Our research reflects Threat Actors, Tools, Client Countries, Customer Sectors, and MITRE ATT&CK Techniques from Q4 of 2021. All of the data around these events, including indicators, YARA rules, and detection logic, are available in MVISION Insights.

MOST REPORTED NATION-STATE MITRE ATT&CK TECHNIQUES

1. PowerShell
2. Scheduled Task
3. Obfuscated Files or Information
4. Windows
5. Web Protocols

▲ 95%

Cobalt Strike ranked highest among Nation-State Threat Tool observations in Q4 2021.

▲ 30%

APT 29 ranked highest among total Nation-State observations in Q4 2021, a 35% increase over Q3.

26%

Nation-State activity in Turkey accounted for 26% of total detections in Q4 2021.

ENTERPRISE CUSTOMER SECTORS

- Telecom
- Transportation and Shipping
- Business Services
- Government
- Non-Profit

PREVALENT THREAT STATISTICS

Our team tracked threat categories in the fourth quarter of 2021. The research reflects percentages of detections in the type of prevalent Malware families observed, associated Client Countries, Enterprise Customer Sectors, and MITRE ATT&CK techniques.

ENTERPRISE CUSTOMER SECTORS

- Transportation
- Telecom
- Consumer
- Business Services
- Technology

75%

RedLine Stealer (20%), Raccoon Stealer (17%), Remcos RAT (12%), LokiBot (12%), and Formbook (12%) amounted to almost 75% of Malware Families Tool Threats observed in Q4 2021.

62%

Transportation customers were targeted the most (62%) among sectors in Q4 2021 – more than the remaining top-10 sector combined.

80%

Rise in observations affecting U.S. clients from Q3 2021.

MOST REPORTED MITRE ATT&CK TECHNIQUES

1. Obfuscated Files or Information
2. Credentials from Web Browsers
3. File and Directory Discovery
4. Registry Run Keys/ Startup Folder
5. System Information Discovery

MOST PREVALENT MALWARE FAMILIES

	RedLine Stealer	Raccoon Stealer	Remcos RAT	LokiBot	Formbook
Q3	1.2%	N/A	24%	19%	36%
Q4	20%	17%	12%	12%	12%

THREATS TO COUNTRIES, CONTINENTS, SECTORS, AND VECTORS

Notable country and continent increases of open-sourced publicly reported incidents in the fourth quarter of 2021 include:

ATTACK VECTORS

- Malware (46%)
- Unknown (19%)
- Account Takeover (16%)
- Vulnerability (10%)
- Targeted Attack (8%)

150%

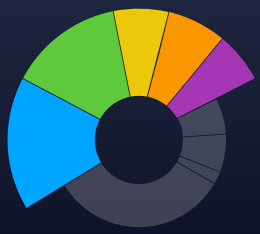
Germany recorded the highest increase (150%) of incidents reported in Q4 2021.

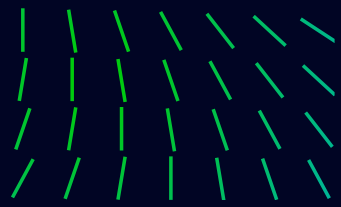
38%

The United States experienced the most reported incidents in Q4 2021 – 38% of total reported incidents.

ATTACK SECTORS

- Individuals
- Healthcare
- Technology
- Public
- Education





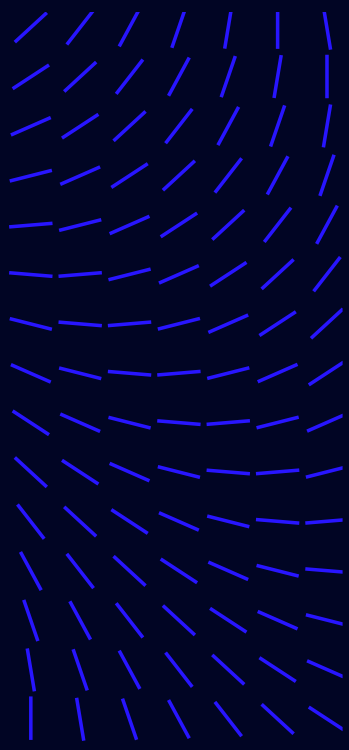
LIVING OFF THE LAND

Cybercriminals continue to develop custom tools but often turn to Living off the Land (LotL) techniques to abuse legitimate binaries and administrative utilities to deliver malicious payloads to a target system. Based on fourth quarter events in 2021, Trellix has identified a slight shift in the trend of tools being used by adversaries as they attempt to remain undetected.

Tactics, Techniques, and Procedures change as defenses strengthen and the security community shares indicators of compromise amongst peers. In our Q3 report we highlighted some of the common Windows binaries that are present on a production system as well as some that are used by administrative staff to perform daily tasks. It was also recommended to deploy necessary machine software, monitor for anomalies, and maintain system efficiencies. Threat actors have taken advantage of usefulness of these utilities for nefarious activities continuing from the Q3 report we look at the utilities abused by threat actors in the fourth quarter and see a slight shift in use. The fact remains: threat actors attempt to remain undetected and are abusing what is already present on a system to deliver payloads including ransomware, beacons, information stealers, and reconnaissance tools.

To identify these binaries or administratively used tools during the reconnaissance phase, adversaries may gather information on technologies used from job postings, customer testimonials advertised by vendors, or from an inside accomplice.

Native OS Binaries		Comments
Windows Command Shell (CMD) (53.44%)	T1059.003	Windows Command Shell is the primary CLI utility for Windows and is often used to execute files and commands in an alternate data stream.
Powershell (43.92%)	T1059.001	PowerShell is often used to execute scripts and PowerShell commands.
WMI/WMIC (33.86%)	T1218, T1564.004	WMIC is a command line interface for WMI and may be used by adversaries to execute commands or payloads locally, in alternate data streams or on a remote system.
Rundll32 (24.34%)	T1218.011, T1564.004	Rundll32 can be used to execute local DLL files, DLL files from a share, DLL files obtained from the internet and alternate data streams.
Regsvr32 (14.29%)	T1218.010	Regsvr32 may be used by adversaries to register dll files, execute malicious code and bypass application whitelisting.
Schtasks (12.70%)	T1053.005	An adversary may schedule tasks that maintain persistence, execute additional malware, or perform automated tasks.



MSHTA (10.05%)	T1218.005	MSHTA may be used by adversaries to execute JavaScript, JScript and VBScript files that may be hidden in HTA files locally and in alternate data streams or retrieved from a remote location.
Excel (8.99%)	T1105	While not natively installed, many systems contain spread sheet software, adversaries may send attachments to user that contain malicious code or scripts that, when executed, may be used to retrieve payloads from a remote location.
Net.exe (7.94%)	T1087 & Sub-techniques	Windows command line utility that allows an adversary to perform reconnaissance tasks such as identifying users, network, and services functionality of a victim machine.
Certutil (4.23%)	T1105, 1564.004 T1027	Windows command utility is used to obtain certificate authority information and configure certificate services. Alternatively, adversaries may use certutil to gather remote tools and content, encode and decode files as well as access alternate data streams.
Reg.exe (3.70%)	1003.002, 1564.004	Reg.exe may be used by adversaries to add, modify, delete, and export registry values which may be saved to alternative data streams. Additionally, reg. exe may be used to dump credentials from a SAM file.

Administrative Tools			Comments
Remote Services (35.98%)	T1021.001, T1021.004, T1021.005	AnyDesk ConnectWise Control RDP UltraVNC PuTTY WinSCP	Remote services tools, both native to Windows and third-party software may be used by adversaries along with valid accounts to gain access to a machine or infrastructure remotely, perform ingress transfer of tools and malware as well as exfiltrate data.
Archive Utilities (6.35%)	T1560.001	7-Zip WinRAR WinZip	Adversaries may use archive utilities to compress collected data in preparation to be exfiltrated as well as to decompress files and executables.
BITSAdmin (3.70%)	T1105, T1218, T1564.004		BiTSAdmin is often used to maintain persistence, clean up artifacts and for invoking additional actions once a set criterion is met.
ADFind (2.65%)	T1016, T1018 T1069, & Sub-Techniques, T1087 & Sub-techniques, T1482		Command line utility that may be used by adversaries to discover active directory information such as Domain Trusts, Permission Groups, Remote Systems and Network Configurations.
PsExec (2.12%)	T1569.002		PsExec is a tool used to execute commands and programs on a remote system.
fodhelper.exe (0.05%)	T1548.002		Fodhelper.exe is a Windows utility that may be used by adversaries to run malicious files with elevated privileges on a victim machine.

RESOURCES

To keep track of the latest threats and research, see these Trellix resources:

Threat Center – Today's most impactful threats identified by our team.

TWITTER

Trellix Threat Labs

Christiaan Beek

John Fokker

Douglas McKee

Steve Povolny

DOWNLOAD PDF

View Threat Report Archives

ABOUT TRELLIX

Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers. More at www.trellix.com.

Trellix Threat Labs

Subscribe to Receive Our Threat Information

WRITING AND RESEARCH

Christiaan Beek
Tim Hux
John Fokker
Douglas McKee
Tim Polzer
Steve Povolny
Leandro Velasco
Max Kersten
Alfred Alvarado
Thibault Seret

Trellix

6220 American Center Drive,
San Jose, CA 95002