Top-targeted vulnerabilities & Email threats

Top vulnerabilities, email lures and tools to gain access

Cisco Talos observed many ways in which cybercriminals targeted people and systems in 2024. For further analysis and additional research, download Talos' full 2024 Year in Review report.

Vulnerabilities affecting EOL devices are among most targeted network device CVEs

Talos looked at the top-targeted network device vulnerabilities to see what types of devices attackers are prioritizing in their operations. Many of these vulnerabilities are ubiquitous in systems globally and have largely been exploited by known botnets, which can establish control over the compromised devices and launch large-scale disruptive attacks. Because of the access that routers, firewalls, and other network devices afford, their compromise can easily allow an attacker to move laterally, carry out other phases of their attacks, and potentially take over entire networks.

Notably, some of these top-targeted vulnerabilities affect end-of-life (EOL) devices and therefore have no available patches, despite being actively targeted by threat actors.

Email threats

Talos saw adversaries gain initial access via phishing in nearly a quarter of Talos Incident Response (IR) incidents. In those cases, embedded malicious links appeared to be more successful than other modes of phishing, like email attachments or voice phishing (vishing).

Actors use simple subject lines in phishing lures but still leverage major events

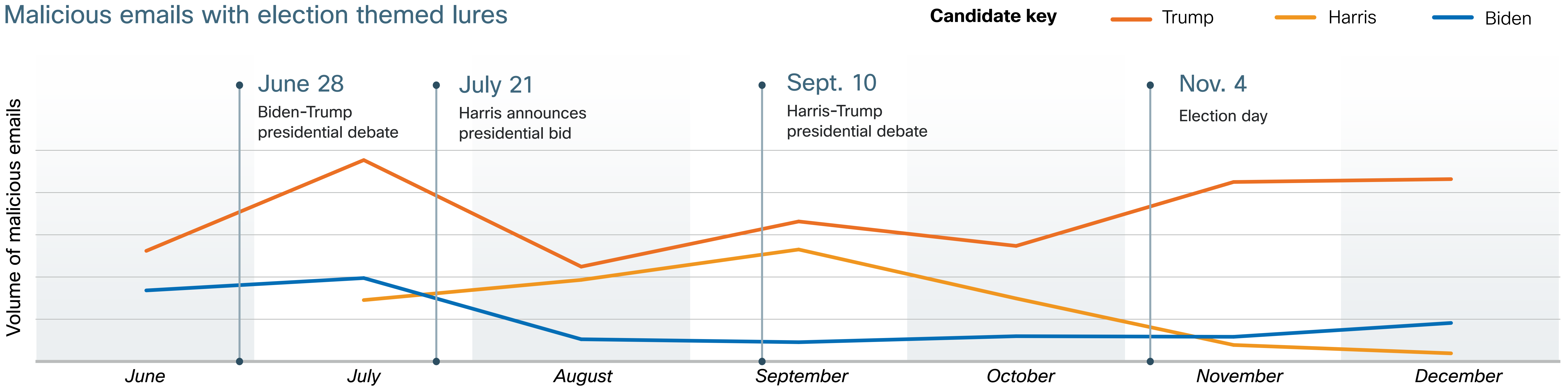
In 2024, threat actors largely abandoned the use of urgent or time-sensitive subjects in their lures, instead opting for terms that are far less sensational and perhaps more likely to be mistaken as benign messages. However, Talos also saw evidence that threat actors remain attuned to major national events, quickly incorporating those themes into phishing lures and spam email to get higher click rates.

Top 10 most targeted network device vulnerabilities

🟧 Denotes EOL product

CVE	Manufacturer	Product	Device type	Vulnerability description
CVE-2024-24919	Check Point	Quantum Security Gateways	Firewall/VPN	Attacker can read sensitive data like password hashes.
CVE-2024-3273	D-Link	Multiple NAS Devices	Network attached storage (NAS)	Allows attacker to execute arbitrary base 64-encoded commands on the devices.
CVE-2024-3272	D-Link	Multiple NAS Devices	Network attached storage (NAS)	Allows attacker to execute arbitrary base 64-encoded commands on the devices.
CVE-2023-1389	TP-Link	Archer AX21	Router	Attacker can inject commands, which would be run as root, with a simple POST request.
CVE-2024-3400	Palo Alto Networks	PAN-OS	Firewall	Gives attacker ability to execute commands with root privileges on the firewall.
CVE-2023-36845	Juniper	Junos OS	Network device software	Attacker can inject and execute malicious code.
CVE-2021-44529	Ivanti	Endpoint Manager Cloud Service Appliance	Endpoint device manager	Allows attacker to execute malicious code with limited permissions.
CVE-2023-38035	Ivanti	Ivanti Sentry	Security gateway	Allows attacker to access sensitive API data and configurations, run system commands, or write files onto the system.
CVE-2024-36401	OSGeo	GeoServer	Server	Attacker can conduct remote code execution via specially crafted input.
CVE-2024-0012	Palo Alto Networks	PAN-OS	Firewall	Allows attacker to gain administrator privileges.

Malicious emails with election themed lures



Most used tools

Interested in the full report? Download here

LoLBins were the most prevalently used tools, enabling actors to blend in with normal traffic

Living-off-the-land binaries (LoLBins) – or tools and utilities found natively on an endpoint – were used the most often across Talos IR engagements, alongside many different commercial and open-source tools. LoLBins are effective because they allow a threat actor to carry out various stages of their operation, often without using additional malware, external tools, or exploits. Most importantly, malicious activity emanating from LoLBins is hard to detect since these tools and utilities are used legitimately in daily operations.

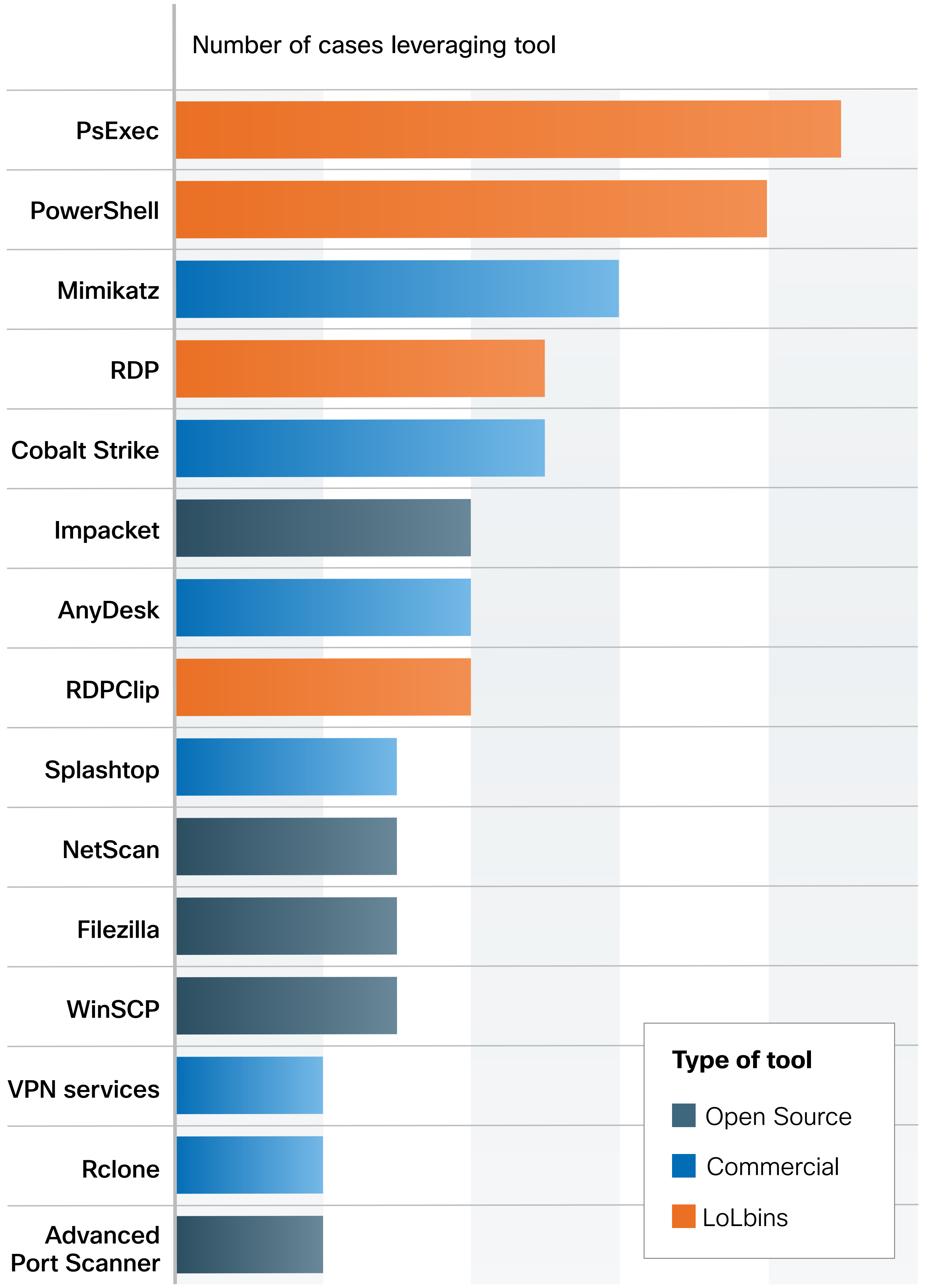
Common LoLBins, such as PSExec, PowerShell, and remote desktop protocol (RDP) are just three of the top five tools that were used to facilitate large components of an adversary's attack chain.

Since organizations regularly use many of these tools to support daily operations, it can be difficult to discern when their use or presence on an endpoint might be nefarious. The figure below shows how the most commonly seen tools in Talos IR cases from each category are intended to be used, and how actors are coopting them for their own malicious purposes.

Use and abuse of most common tools in Talos IR cases

	PsExec	Impacket	Mimikatz
Intended use	Part of Microsoft's Sysinternals suite of tools; allows users to run commands on local and remote systems.	Open-source Python library for performing network audits.	A credential-dumping utility commonly used by penetration testers and red teams to extract plain text passwords.
Malicous capabilities	Has the ability to execute processes on other systems remotely, remotely create accounts on target systems, download or upload a file over a network share.	Impacket modules like SecretsDump allow actors to steal account and password information from Active Directory databases.	Contains functionality to acquire information about credentials, including from LSASS memory, registry hives, DPAPI, among others.
Threat actor abuse	Many ransomware operations use PsExec to run their payload on all systems in the domain.	APTs and other actors frequently use Impacket to gain a foothold in the victim environment and move laterally.	Cybercriminals to APT groups use Mimikatz to steal account logins and credentials to aid in moving laterally in the victim environment.

LoLBins used across the attack chain in Talos IR incidents


Number of cases leveraging tool
PsExec
PowerShell
Mimikatz
RDP
Cobalt Strike
Impacket
AnyDesk
RDPClip
Splashtop
NetScan
Filezilla
WinSCP
VPN services
Rclone
Advanced Port Scanner
Type of tool
Open Source
Commercial
LoLbins