

The Growing Threat of ShadowPad Malware and Its Business Impact

 cyberint.com/blog/dark-web/the-growing-threat-of-shadowpad-malware-and-its-business-impact

Adi Bleih

June 24, 2026



EXPOSURE MANAGEMENT

The Growing Threat of ShadowPad Malware and Its Business Impact



Dark Web

Introduction to ShadowPad Malware

ShadowPad, a sophisticated modular malware, has emerged as a significant cybersecurity threat. Attributed initially to Chinese state-sponsored threat actors (APT41), this malware has evolved into a shared tool among various APTs. Its highly customizable nature allows attackers to adapt ShadowPad to specific targets, making it a versatile and persistent threat. The malware's design emphasizes stealth and modularity, enabling it to execute various malicious activities, including data exfiltration, lateral movement, and backdoor operations.

ShadowPad first appeared in 2015 as the successor to PlugX. However, it gained significant public attention only after being linked to high-profile supply-chain attacks, including CCleaner, NetSarang, and ShadowHammer. Unlike PlugX, which was publicly available for purchase, ShadowPad is exclusively shared among a restricted group of users.

Delivery Methods of ShadowPad Malware

ShadowPad is a modular backdoor in shellcode format. During its execution, an obfuscated shellcode loader decrypts and loads a root plugin. This root plugin, in turn, decrypts and loads additional plugins embedded within the shellcode into memory.

A compelling question arises: is ShadowPad a privately shared attack framework or a custom-built modular malware platform designed for exclusive sale to specific groups? Its architecture enables users to remotely deploy new plugins to the backdoor. In theory, anyone capable of creating a plugin encrypted and compressed in the correct format can freely extend the backdoor's functionality.

However, the plugin control interfaces are hardcoded into the "Manager" page of the ShadowPad controller. Notably, the controller lacks a feature to add new control interfaces.

Beyond the plugins embedded in the sample, additional plugins can be remotely uploaded from the C&C server, allowing users to dynamically expand its functionality beyond the default set.

ShadowPad employs multiple delivery mechanisms tailored to exploit specific vulnerabilities and target environments. These methods include:

1. **Software Supply Chain Attacks:** ShadowPad has been deployed via compromised updates of legitimate software. For example, attackers have inserted malicious code into software updates for widely used enterprise applications. This method exploits the inherent trust in software vendors, making detection and prevention highly challenging.
2. **Exploitation of Vulnerabilities:** Threat actors leveraging ShadowPad frequently exploit unpatched vulnerabilities in enterprise software or network infrastructure. These vulnerabilities include zero-day exploits and known issues for which patches are available but not yet applied.
3. **Spear-Phishing Campaigns:** Carefully crafted phishing emails are another standard delivery method. These emails often contain malicious attachments or links that, when opened, execute scripts to download and install ShadowPad on the target's system.
4. **Living-off-the-Land (LotL) Techniques:** ShadowPad operators often use legitimate administrative tools and scripts to deliver the malware. By leveraging tools like PowerShell or Windows Management Instrumentation (WMI), they reduce the likelihood of detection by security systems.
5. **Compromised Websites and Watering Hole Attacks:** In some cases, ShadowPad has been distributed via websites frequented by specific targets. These watering hole attacks compromise legitimate websites to serve malware to unsuspecting visitors.

The Impact of ShadowPad Malware

The deployment of ShadowPad can have severe consequences for targeted organizations. Its impact includes:

1. **Data Exfiltration:** ShadowPad is adept at stealing sensitive data, including intellectual property, customer information, and financial records. This stolen data can be used for espionage or sold on underground markets.
2. **Operational Disruption:** By enabling lateral movement and persistence, ShadowPad can disrupt normal operations. Its ability to install additional payloads or disable critical systems can result in downtime and financial losses.
3. **Espionage:** Given its roots in state-sponsored cyber activities, ShadowPad is often used for intelligence-gathering. It has been linked to campaigns targeting government institutions, critical infrastructure, and high-value corporate assets.
4. **Financial Losses:** The costs associated with ShadowPad attacks can be significant. These include expenses for incident response, system recovery, and potential regulatory fines for data breaches.
5. **Reputational Damage:** Organizations targeted by ShadowPad may suffer reputational harm, losing customer trust and market value. Public disclosure of such incidents often results in negative press coverage and long-term damage to brand reputation.

About Check Point Exposure Management

Check Point Exposure Management is an intelligence-led, validation-driven, remediation-first unified platform that helps security teams move quickly and safely from exposure visibility to exposure reduction. Delivered through a single UI, it brings together threat intelligence, exposure prioritization, Agentic Exposure Validation, and safe remediation so teams can understand risk, prove exploitability, and act from one place.

[Schedule Your Demo Now](#)

ShadowPad Malware TTPS

Tactic Name	Technique
Lateral Movement	T1021.002 – SMB/Windows Admin Shares
Persistence	T1574.002 – DLL Side-Loading
Privilege Escalation	T1574.002 – DLL Side-Loading

Tactic Name	Technique
Defense Evasion	T1574.002 – DLL Side-Loading
Lateral Movement	T1550.002 – Pass the Hash
Defense Evasion	T1550.002 – Pass the Hash
Defense Evasion	T1218.011 – Rundll32
Execution	T1059.001 – PowerShell
Execution	T1203 – Exploitation for Client Execution
Command and Control	T1568.002 – Domain Generation Algorithms
Defense Evasion	T1027.011 – Fileless Storage
Privilege Escalation	T1055.001 – Dynamic-link Library Injection
Defense Evasion	T1055.001 – Dynamic-link Library Injection
Command and Control	T1105 – Ingress Tool Transfer
Command and Control	T1568.002 – Domain Generation Algorithms
Discovery	T1082 – System Information Discovery
Privilege Escalation	T1055 – Process Injection
Defense Evasion	T1055 – Process Injection
Command and Control	T1071.001 – Web Protocols
Defense Evasion	T1027 – Obfuscated Files or Information
Command and Control	T1095 – Non-Application Layer Protocol
Command and Control	T1071.002 – File Transfer Protocols
Command and Control	T1132.002 – Non-Standard Encoding
Command and Control	T1071.004 – DNS
Discovery	T1057 – Process Discovery

Tactic Name	Technique
Exfiltration	T1029 – Scheduled Transfer
Discovery	T1016 – System Network Configuration Discovery
Defense Evasion	T1140 – Deobfuscate/Decode Files or Information
Defense Evasion	T1070 – Indicator Removal
Discovery	T1124 – System Time Discovery
Defense Evasion	T1112 – Modify Registry
Discovery	T1033 – System Owner/User Discovery

ShadowPad Malware IOCs (Sample 50)

Type	Date Added	Value
SHA-256	2026-05-02	a53a03026dd4efe462769a6e8d648454efcf53d40eb765bae506249baf4d74c5
URL	2026-04-16	http://o.casasferiasacores.org/forum/viewtopic.php
URL	2026-04-16	http://o.cutanddrop.com/forum/viewtopic.php
SHA-256	2026-04-15	805b1dbf373986fb98f346b491cea9ce75c44ea7cc55339260c344606773e236
SHA-256	2026-02-25	2c0a31962b535dcf0ffd10f646ccf0549b0792d3aa3bd7405a8712f097f41d31
URL	2026-02-23	http://eyota.com.sg/group/panelnew/gate.php
SHA-256	2026-02-22	0f0f59593cfae8f5fb3d1ab9af840348c2866a8bddf95be8f98cb7e8874b1138

Type	Date Added	Value
URL	2026-02-11	http://www.ttghk.com/malyka/panel/gate.php
SHA-256	2026-02-10	d0ba595dc1afd4ea3c1aad23d2bb5e3652853b56f8358a853f41e164d4bb1f97
URL	2026-01-23	http://66.175.216.33/forum/viewtopic.php
MD5	2026-01-23	203dd619f92192331f488854ccde6178
SHA-1	2026-01-23	4811f317e933d13961b9cc8b38d41d4fae67dcc5
SHA-256	2026-01-22	9db343a12b7b22ba7feca33019a437067f96e03a2695f574a97f446f7dc2883b
URL	2026-01-21	http://thesavvyplayer.com/images/view.php
IPv4 Addresses	2025-11-30	196.196.41.173
URL	2025-11-30	https://196.196.41.173/admin.php
URL	2025-11-24	http://file.filecrate.ru/bussin/gate.php
SHA-256	2025-11-23	3ab0c58f330345f3dae67a4f68a4b1b4e4b8ae975aa82d90f9b013200ed4f8b0
URL	2025-10-12	http://www.ronaldsay-holdings.com/zd2.exe
URL	2025-10-12	http://www.airtime-telecom.co.uk/QKe0W2o.exe

Type	Date Added	Value
URL	2025-10-12	http://schnell-ordner.de/W9etP.exe
URL	2025-10-12	http://mutantchicken.co.uk/8HT5Hv4F.exe
URL	2025-10-12	http://agroos.com/VnDMm.exe
URL	2025-10-11	http://50.116.57.82/ponyb/gate.php
URL	2025-10-10	http://solarstorez.com/lambo/panel/shit.exe
SHA-256	2025-10-08	d49288276e163a4ebf7d2557428a91278751a05843493171e90df3257bf217be
URL	2025-10-08	http://central.pk/corporate/enter/joe/gate.php
SHA-256	2025-10-07	121a8901094eb205730a3a7f3e176335bf000600c2af96e75c887d61b5e1fbe3
URL	2025-10-04	http://gunesyapiurunleri.com/bayi/.menu/cache/info/network.php
MD5	2025-09-16	2f2988f95692d3119e50f174619653a1
SHA-1	2025-09-16	c903f04c22f19d32bdf76bbd9ef4a8c98befaa7d
URL	2025-09-15	http://eyota.com.sg/a2z/panelnew/gate.php
SHA-256	2025-09-14	0380c01d290b6b77769d1494aa19fea1b893446a0048330314a93b695f0ec1dd

Type	Date Added	Value
SHA-256	2025-09-10	031e095f10661205df66520a7bedd5414e2b4b1aa132bc615c4f9bc8f04f2d70
URL	2025-09-10	http://theonlygoodman.com/ded/gate.php
URL	2025-09-03	http://www.kitchenaria.com/modules/gateway2/Protx/response.php
URL	2025-09-03	http://forums.lolapps.com/includes/cron/response.php
SHA-256	2025-09-02	0ad0298b4303962d0cf5a392ca2c3ad4bd2cd1d857c7a4810a0d1129888773ac
URL	2025-09-02	http://fwcpafl.com/dam/ponnie/gate.php
URL	2025-09-02	http://pony.gsghost.pro/panel/gate.php
URL	2025-09-02	http://pony.gsghost.pro/panel/shit.exe
URL	2025-08-31	http://u90886cz.beget.tech/gate.php
SHA-1	2025-08-31	ec53ba9e3842881124551006f72bebb9635d92eb
MD5	2025-08-31	2522ee98eb3ea294c9813948111b938b
SHA-256	2025-08-30	1c2b79b3d719dc91f95394c2dbfe8149610ffa668eadec4c491000882dc3b761
URL	2025-08-27	http://gbg.gr/kb/cboi9822/gate.php

Type	Date Added	Value
SHA-1	2025-08-27	e7c46f5a16730d0242bcf264659db4e101028b57
MD5	2025-08-27	3afc4d466ea35fcb15cff7b23a7ed399
SHA-256	2025-08-26	c0cb68c9404c00ab57d203c257621cbb77548c7ff6a322fa994f9e79b30f7cf8
SHA-256	2025-08-26	d0c8596e72059a5c5e5421929f65efbeebca319d1227fd2e1db89f9117ae7c55d