

The Rise of Pony Malware and What it Means for Organizations

 cyberint.com/blog/dark-web/the-rise-of-pony-malware-and-what-it-means-for-organizations

Adi Bleih

June 14, 2026



Dark Web

Introduction to Pony Malware

Pony, also recognized as Fareit or Siplog, operates as an information stealer and loader, serving as malware designed to gather data from compromised systems and facilitate the installation of other malicious programs. This particular virus made its initial appearance in the wild in 2011, primarily targeting users in Europe and North America.

The earliest identified iteration of Pony stealer is version 1.7, with the most recent known version being 2.2. Despite regular updates, the malware has not undergone groundbreaking feature enhancements since its initial discovery by Microsoft. In addition to its core functionality, Pony possesses the capability to pilfer credentials from cryptocurrency wallets, FTP clients, and autofill values stored in browsers.

Diverging from the typical botnet structure, Pony stealer does not rely on a centralized Command and Control (C&C) server or a network of such servers for executing its attacks. Instead, each attacker can establish a customized control server or acquire a server

previously configured by another malefactor, instantly gaining access to infrastructure that generates reports on the pilfered data. Furthermore, the malware itself comprises two modules: the builder, used to construct clients downloadable onto victims' machines for data collection, and the bot, representing the final payload.

Deep Dive into Pony Malware

The Pony stealer builder functions as a tool for attackers to construct tailored Pony bots with pre-programmed C&C addresses for sending stolen data. The Pony Bot, the actual program responsible for information theft, is predominantly written in assembly language. A distinctive feature setting this malware apart is its unique decoding technique—the Bot lacks an embedded decoding algorithm and relies on simple functions programmed to transmit encrypted information to the control server, where the stolen data undergoes decryption.

Part of Pony's notoriety stems from the leakage of the source code for multiple versions of Pony loader, available for download on darknet platforms. Notably, the source code for Pony builder and loader versions 1.9 and 2.0 can be found on several underground forums.

Despite the core features of the Pony trojan remaining relatively consistent over its lifespan, newer versions have incorporated several anti-detection features to impede research and disassembly. In addition to standard anti-evasion and debugging techniques, attackers can implement various packers, including custom ones, to thwart detection by antivirus software.

Delivery Methods of Pony Stealer Malware

Pony is distributed through diverse channels, including email spam campaigns, exploit kits, and DNS poisoning. Additionally, it can be concealed within free downloadable online programs, masquerading as legitimate software. For instance, malicious emails often contain either a Microsoft Word archive or a JavaScript file. Upon downloading and opening the document, Pony infiltrates the victim's PC and initiates its execution.

Another avenue of Pony's attack involves compromising a DNS server infected by another malware. In this scenario, the victim is redirected to a malicious website, from which Pony is downloaded onto the user's PC.

Impact of Pony Malware

The widespread availability and robust feature set have positioned Pony stealer as one of the most prevalent information stealers. It is frequently utilized in attacks targeting Europe and

North America, posing an enhanced threat due to its nesting-doll-like design, where the final payload resides within a layered package, facilitating evasion of easy detection.

Researchers note that Pony Stealer functions as a potent password stealer, capable of decrypting or unlocking passwords for over 110 different applications, encompassing VPNs, FTP clients, email services, instant messaging platforms, web browsers, and more. Once Pony Stealer infects a PC, it transforms the device into a botnet, leveraging the infected PCs to propagate further infections.

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](#)

Pony Malware TTPs

Tactic	Technique
Defense Evasion	T1070.004 File Deletion
Credential Access	T1110.001 Password Guessing
Discovery	T1087.001 Local Account
Initial Access	T1566.001 Spearphishing Attachment
Command and Control	T1071.001 Web Protocols
Execution	T1204.001 Malicious Link
Defense Evasion	T1497.003 Time Based Evasion
Discovery	T1497.003 Time Based Evasion
Discovery	T1082 System Information Discovery

Tactic	Technique
Initial Access	T1566.002 Spearphishing Link
Defense Evasion	T1027 Obfuscated Files or Information
Execution	T1059.003 Windows Command Shell
Command and Control	T1105 Ingress Tool Transfer
Defense Evasion	T1036.005 Match Legitimate Name or Location
Execution	T1204.002 Malicious File
Execution	T1106 Native API

Pony Malware IOCs (Sample of 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	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.gsgghost.pro/panel/gate.php
URL	2025-09-02	http://pony.gsgghost.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