

URSNIF, EMOTET, DRIDEX and BitPayme Linked by Loader

By Trend Micro Research Dec 18, 2018 Read time: 3 min (827 words)

Published: 2018-12-18 · Archived: 2026-04-05 13:27:36 UTC

As ransomware and [banking trojans](#) captured the interest – and profits – of the world with their destructive routines, cybersecurity practitioners have repeatedly [published news- cybercrime-and-digital-threats online open on a new tab](#) and [offline](#) how [cybercriminals](#) have compartmentalized their schemes through exchange of information and banded professional organizations. As a more concrete proof of the way these symbiotic relationships and work flows intersect, we discovered a connection between [EMOTET](#), [URSNIF](#), [DRIDEX](#) and [BitPaymer](#) from open source information and the loaders of the samples we had, functioning as if tasks were divided among different developers and operators.



Figure 1. Connections of EMOTET, DRIDEX, URSNIF and BitPaymer.

Background and details

In order to have a better understanding of the significance of these connections, here's a summarized background of each malware family:

- URSNIF / [GOZI-ISFB](#)

Still considered as one of the global top threats, this banking trojan's source code was among those [repeatedly leaked news- cybercrime-and-digital-threats](#) because of its evolution and [notoriety for adaptive behaviors](#). This spyware monitors traffic, features a keylogger, and steals credentials stored in browsers and applications. The malware creators of GOZI admitted to its creation and distribution, and was [sentenced in 2015 and 2016 open on a new tab](#).

- DRIDEX

Another banking trojan that [targets banking and financial institutions](#), the cybercriminals behind it use various methods and techniques to steal personal information and credentials through malicious attachments and HTML injections. DRIDEX evolved from [CRIDEX](#), [GameOver Zeus](#) and [ZBOT](#), and [proved to be resilient](#) even after it was momentarily taken down in 2015 through [a partnership with the FBI](#).

- EMOTET

Discovered by [Trend Micro in 2014](#), this malware acts as a loader for payloads such as [Gootkit](#), [ZeusPanda](#), [IcedID](#), [TrickBot](#), and DRIDEX for critical attacks. Other publications have also [mentioned](#) observing obfuscation techniques between EMOTET and URSNIF/GOZI-ISFB.

- BitPaymer

This ransomware was used to [target medical institutions](#) via remote desktop protocol and other email-related techniques, momentarily shutting down routine services for a high ransom. Security [researchers](#) later published evidence that not only was [DRIDEX dropping BitPaymer](#), but that it also came from the [same cybercriminal group](#).

During our analysis, we found evidence that the malware families identified had shared loaders: the overview of the payload decryption procedure, and the loaders' internal data structure. While the first figure of the disassembled PE packers had small differences in their arithmetic operations' instructions, we found that the four payload decryption procedures were identical in data structures' overview on the way they decrypted the actual PE payloads.



Figure 2. Overview of identical structures of payloads' loader decryption procedures.

Further analysis also revealed that the internal data structure of the four malware families were the same. We compared the disassembled codes from the samples we had and noticed the encrypted payload address and size placed into the decryption procedure located at offset 0x34 and 0x38.



Figure 3. Identical data structures show similar payload addresses and sizes.



Figure 4. Data structure used by the shared loader.

As cybercrime organizational structures in some countries tend to compartmentalize work, we suspect that the four malware families' gangs might be in contact with the same weapon providers for PE loaders. In addition, it's also possible that these four cybercrime groups may establish some attributional – working or otherwise – relationships and have exchanged or continue to exchange resources.

In our history of monitoring botnets and the underground organizations who make and/or use them, the cybercriminals behind [EMOTET may be sharing to collaborate with trusted, highly-skilled cybercriminal groups](#), and may be a sign of these four groups' ongoing and intriguing relationship.

Alliances like these could lead to more destructive malware deployments in the future. More than ever, it is important for organizations to heighten cybersecurity preventive measures, such as establishing policies and procedures for handling security threats. Regular education awareness sessions and reminders for employees can help protect the enterprise from attacks and intrusions from malicious emails and URLs. Installing and updating a multi-layered protection and solution in preventing online banking threats can go a long way in securing businesses.

Trend Micro Solutions

Trend Micro endpoint solutions such as the [Smart Protection Suites](#) products and [Worry-Free Business Security](#) solutions can protect users and businesses from threats by detecting malicious files and messages as well

as blocking all related malicious URLs. [Trend Micro™ Deep Discovery™ products](#) has an email inspection layer that can protect enterprises by detecting malicious attachments and URLs.

Trend Micro XGen™ security provides a cross-generational blend of threat defense techniques to protect systems from all types of threats, including ransomware and cryptocurrency-mining malware. It features high-fidelity [machine learning](#) on gateways and endpoints, and protects physical, virtual, and cloud workloads. With capabilities like web/URL filtering, behavioral analysis, and custom sandboxing, XGen security can secure systems against modern threats that bypass traditional controls; exploit known, unknown, or undisclosed vulnerabilities; either steal or encrypt personally identifiable data; or conduct malicious cryptocurrency mining. Smart, optimized, and connected, XGen security powers Trend Micro's suite.

Indicators of Compromise

Malware	SHA256
URSNIF	9d38a0220b2dfb353fc34d03079f2ba2c7de1d4a234f6a2b06365bfc1870cd89
DRIDEX	cbd130b4b714c9bb0a62e45b2e07f3ab20a6db3abd1899aa3ec21f402d25779e
EMOTET	0a47f5b274e803754ce84ebd66599eb35795fb851f55062ff042e73e2b9d5763
BitPaymer	d693c33dd550529f3634e3c7e53d82df70c9d4fbd0c339dbc1849ada9e539ea2

Source: <https://blog.trendmicro.com/trendlabs-security-intelligence/ursnif-emotet-dridex-and-bitpaymer-gangs-linked-by-a-similar-loader/>