LevelBlue - Open Threat Exchange

By CODERED_VTA

Archived: 2026-04-02 11:41:38 UTC

- 54 Subscribers

Phorpiex - Downloader Delivering Ransomware

CVE: 1 | **FileHash-MD5:** 6 | **FileHash-SHA1:** 6 | **FileHash-SHA256:** 7 | **URL:** 5 | **Domain:** 1 | **Email:** 2

A report by Cybereason Security Services looks at the connection between the LockBit ransomware group and the Phorpiex botnet, a notorious cybercrime group that has been active since 2010.

- 840 Subscribers

- 258 Subscribers

Phorpiex - Downloader Delivering Ransomware

FileHash-MD5: 5 | **FileHash-SHA1:** 4 | **FileHash-SHA256:** 6 | **URL:** 4 | **Domain:** 1 | **Email:** 2

The report analyzes the Phorpiex botnet's role in delivering LockBit Black Ransomware. It highlights the automated execution of ransomware through Phorpiex, minimal changes to the botnet's code since its source code sale in 2021, and direct deployment of LockBit without network expansion. The analysis covers the infection flow, phishing emails, and technical details of different Phorpiex variants. Key features include URL cache deletion, library obfuscation, indicator removal, and persistence mechanisms. The report also provides a comparative analysis of LockBit, GandCrab, and TWIZT downloader variants, along with IOCs and MITRE ATT&CK mapping.

- 373,196 Subscribers

Ransomware Indicators of Compromise (IOC) Feed - PrecisionSec

FileHash-MD5: 10 | **FileHash-SHA1:** 9 | **FileHash-SHA256:** 9

PrecisionSec is the world’s leading cyber security firm and is offering a 30-day free trial of malware detection and blocking the most prolific and dangerous threat in today's landscape, including ransomware.

- 0 Subscribers

Aiming at domestic government and enterprises! Deeply revealed ransomware operator Rast gang

FileHash-MD5: 10 | **FileHash-SHA1:** 5 | **FileHash-SHA256:** 5 | **Email:** 12

A new ransomware threat, dubbed Rast, has emerged targeting Chinese government and enterprises since December 2023. Written in Rust, Rast has infected over 6,800 terminals, successfully encrypting more than 5,700. The Rast gang, named after the ransomware, operates primarily between 20:00 and 05:00, suggesting a European base. Their attack method involves RDP brute-forcing and exploiting Nday vulnerabilities to access border servers, followed by manual deployment of ransomware components. The gang's tactics are reminiscent of operators distributing Buran, GlobeImposter, Phobos, and GandCrab ransomware. Rast ransomware has evolved through three versions, with the latest requiring manual operation via a console interface. Victim information is uploaded to a MySQL database, revealing a wide range of affected sectors including government, finance, and various industries.

- 373,196 Subscribers

- 1,582 Subscribers

Global- Injection | Phone service modification campaign - Cryprsoft

FileHash-MD5: 626 | **FileHash-SHA1:** 539 | **FileHash-SHA256:** 1335 | **SSLCertFingerprint:** 2 | **URL:** 220 | **Domain:** 501 | **Email:** 4 | **Hostname:** 617

Malicious» http://www.forensickb.com/2013/03/file-entropy-explained.html | Cryptsoft | ET , Virus:Win32/Sality.AT , Win32:Kukacka , TrojanSpy:Win32/Nivdort.AJ , Worm:Win32/Mydoom.O!backdoor , Worm:Win32/Bloored , TrojanSpy:Win32/Invader.S!MSR , Text: Mydoom spreading via SMTP 29 192.168.56.110 198.133.159.125 2018340 ET TROJAN Win32.Sality-GR Checkin 192.168.56.110 52.28.249.128 2018340 ET TROJAN Win32.Sality-GR Checkin 192.168.56.110 166.78.145.90 2016803 ET TROJAN Known Sinkhole Response Header 166.78.145.90 192.168.56.110 2018 ATT&CK | Query Registry , Modify Existing

Service , Scheduled Task/Job , Process Injection , Registry Run Keys / Startup Folder , System Information Discovery , Disabling Security Tools , Modify Registry

- 224 Subscribers

urlhaus.abuse.ch

CVE: 9 | **FileHash-MD5:** 3 | **FileHash-SHA1:** 8 | **URL:** 7927 | **Domain:** 119 | **Hostname:** 162

- 1 Subscribers

- 224 Subscribers

AT&T • Ransom:Win32/GandCrab.AE

FileHash-MD5: 231 | **FileHash-SHA1:** 217 | **FileHash-SHA256:** 1628 | **URL:** 298 | **Domain:** 1047 | **Email:** 7 | **Hostname:** 877

*Edit: I meant to mean at&t may be unaware despite reported outage. My AT&T study is private and researched from corporate device. GandCrab : GandCrab was a Ransomware-as-a-Service (RaaS). GandCrab Ransomware is a ransomware is a malware that asks the victim to pay money in order to restore access to encrypted files. If the user does not cooperate the files are forever lost.In many instances, files are encrypted to control, spy, monitor dns traffic, download other malware, spy on targets, modify, delete, write on victims devices going undetected.

- 218 Subscribers

AT&T • Ransom:Win32/GandCrab.AE

FileHash-MD5: 231 | **FileHash-SHA1:** 217 | **FileHash-SHA256:** 1628 | **URL:** 298 | **Domain:** 1047 | **Email:** 7 | **Hostname:** 877

GandCrab : GandCrab was a Ransomware-as-a-Service (RaaS). GandCrab Ransomware is a ransomware is a malware that asks the victim to pay money in order to restore access to encrypted files. If the user does not cooperate the files are forever lost.In many instances, files are encrypted to control, spy, monitor dns traffic, download other malware, spy on targets, modify, delete, write on victims devices going undetected.

- 218 Subscribers

AT&T • Ransom:Win32/GandCrab.AE

FileHash-MD5: 231 | **FileHash-SHA1:** 217 | **FileHash-SHA256:** 1628 | **URL:** 298 | **Domain:** 1047 | **Email:** 7 | **Hostname:** 877

GandCrab : GandCrab was a Ransomware-as-a-Service (RaaS). GandCrab Ransomware is a ransomware is a malware that asks the victim to pay money in order to restore access to encrypted files. If the user does not cooperate the files are forever lost.In many instances, files are encrypted to control, spy, monitor dns traffic, download other malware, spy on targets, modify, delete, write on victims devices going undetected.

- 218 Subscribers

AT&T • Ransom:Win32/GandCrab.AE

FileHash-MD5: 231 | **FileHash-SHA1:** 217 | **FileHash-SHA256:** 1628 | **URL:** 298 | **Domain:** 1047 | **Email:** 7 | **Hostname:** 877

*Edit: I meant to mean at&t may be unaware despite reported outage. My AT&T study is private and researched from corporate device. GandCrab : GandCrab was a Ransomware-as-a-Service (RaaS). GandCrab Ransomware is a ransomware is a malware that asks the victim to pay money in order to restore access to encrypted files. If the user does not cooperate the files are forever lost.In many instances, files are encrypted to control, spy, monitor dns traffic, download other malware, spy on targets, modify, delete, write on victims devices going undetected.

- 218 Subscribers

- 224 Subscribers

test

FileHash-MD5: 231 | **FileHash-SHA1:** 217 | **FileHash-SHA256:** 1628 | **URL:** 298 | **Domain:** 1047 | **Email:** 7 | **Hostname:** 877

- 1 Subscribers

- 224 Subscribers

- 218 Subscribers

- 218 Subscribers

Outbreak | https://www.hybrid-analysis.com/

CVE: 10 | **FileHash-MD5:** 563 | **FileHash-SHA1:** 312 | **FileHash-SHA256:** 2529 | **URL:** 2817 | **Domain:** 481 | **Hostname:** 818

I'm being redirected. I'm not sure what if Hybrid Analysis is attacked. It's more likely I'm under attack and being redirected or Hybrid Analysis is an unsafe site.

- 218 Subscribers

Source: https://otx.alienvault.com/browse/pulses?q=tag:GandCrab