KPMG

KPMG Cyber Threat Intelligence Platform

Ursnif - Evolutionary Exploits of a Banking Trojan

Ursnif (aka. Gozi, Dreambot, Gozi-IFSB, Papras, Snifula) is a banking trojan, stealer, and spyware, known to be one of the oldest in malware families. First appeared in 2000, primarily associated to stealing financial information. However, it has evolved to cryptocurrency stealer with new functionalities of persistence & obfuscation for stealth. Due to source code leak in 2015, it has undergone significant code forks leading to several active variants such as Dreambot, IAP, RM2, RM3, and most recently LDR4. Ursnif has been observed across Japan, North America, Europe and Asia, with primary focus on targeting banking institutions, financial services, and government agencies.

Gains initial access through various phishing techniques which includes, macro-enabled maldocs & malicious ISO as their latest attack vector. Once iso is executed, it mounts itself and creates new drive, contains a .LNK file which further executes a batch script alsoOne.bat to call an obfuscated JavaScript file named canWell.js. Further canWell executes tslt.db (Ursnif DLL) through downloaded copy of rundll32.exe. Post execution, malware creates an ActiveX object for creating & retrieving registry data which points to new registry entry that stores the obfuscated base64 encoded data to perform process injection. It also executes pause.exe to remain stealthy for few days. PowerShell commands are used to download Cobalt Strike beacon which creates a process to access LSASS memory to steals credentials & system information including Domain Group, domain controller information using WMI & executes system discovery commands. Exfiltrated data through C2 server via several HTTP POST methods.

Ursnif, an ever-evolving trojan, tends to spread through spam emails. To protect yourself, make sure that your organization's email protection is robust and email attachments only from trusted sources are opened.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Associate Partner,
KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai - 400 011 Phone: +91 22 3989 6000, Fax +91 22 3983 6000.

This document is for e-communication only.

#KPMG josh

home.kpmg/in

Follow us on home.kpmg/in/socialmedia

KPMG

KPMG Cyber Threat Intelligence Platform

Ursnif - Evolutionary Exploits of a Banking Trojan

Indicators of Compromise: IP Addresses	
5.42.199[.]83	211.40.39[.]251
186.7.85[.]71	175.120.254[.]9
45.11.182[.]30	185.189.151[.]38
37.34.248[.]24	79.132.128[.]228
31.214.157[.]31	222.236.49[.]124
194.76.224[.]95	58.235.189[.]192
91.241.93[.]111	175.119.10[.]231
185.95.186[.]58	211.171.233[.]129

Indicators of Compromise: Domains	
reggy506[.]ru	superstarts[.]top
uelcoskdi[.]ru	gameindikdowd[.]ru
superlinez[.]top	jhgfdlkjhaoiu[.]su
superliner[.]top	internetlines[.]in
iujdhsndjfks[.]ru	internetlined[.]com
denterdrigx[.]com	renewbleenergey[.]ru

Indicators of Compromise: Hashes
7023e0216b091e44fa43ef32a4eac096
b243fbf64686efc156a7248db8bac0ec
29882a5867707b532b99a19df982de58
281aae187558092aa15b03e85f21b48c
dc5631de9a17bbdd49df198393609f44
b7fd81b81a969efaca7f8068c77e3dfb
bc339c57f60e71778611eb8b17163af6
5228f29cf6d6f1d767a738f3a0920a45
f552d9efa54139fd5575849969ceb9eb
b289cbeea4392eed4f46fc6d997ab1c2
f7d85c971e9604cc6d2a2ffcac1ee4a3
c6b605a120e0d3f3cbd146bdbc358834
c03f5e2bc4f2307f6ee68675d2026c82
6bb867e53c46aa55a3ae92e425c6df91

Indicators of Compromise: Hashes
6a4356bd2b70f7bd4a3a1f0e0bfec9a4
60375d64a9a496e220b6eb1b63e899b3
3db94cf953886aeb630f1ae616a2ec25
d99cc31f3415a1337e57b8289ac5011e
a1f634f177f73f112b5356b8ee04ad19
8ea6ad3b1acb9e7b2e64d08411af3c9a
426649c2297928ed6d6a397cb4db8dabcc25ecee
e78f1e3f668d76e9ecb600562f486647e331c33
411dbca8616af404bb7899fab1f2f03c00dd6798
00b22be8e19e8c5f27f6bd5ce8399e5958560dd2
ffa40314972d310cbf3f1ef803fc378bef377016
6e3315e91e3f7a9378989a5a15d3b15849a098e8
a7128b7d2d33376598ddbca3edc313df7f36ce63
81e41245364ed58b01c7ce09842124dd35724d7f
97ad8c8998669ed2ef381036a75faa531c959bab
dca61b63814428dc1bb246c1acbab4b03e59e5a5
67175143196c17f10776bdf5fbf832e50a646824
328afa8338d60202d5519191 2eea6151f80956d3
4ce65da98f0fd0fc4372b97b3e6f8fbeec32deb3
6d4f1a9658baccd2e406454b2ad40ca2353916ab
485a179756ff9586587f8728e173e7df83b1ffc3
d1b2dd93026b83672118940df78a41e2ee02be80
743128253f1df9e0b8ee296cfec17e5fc614f98d
f67ce90f66f6721c3eea30581334457d6da23aac
7c82b558a691834caf978621f288af0449400e03
7c04c4567b77981d0d97d8c2eb4ebd1a24053f48
fcf194e2fa3bacb8ee950e8da5f02f93c82702607bb6b97def05b215c3f47083
4101cab81e757fa62ac9cb4bdd0d3102e5be0796ceec17b4a5b04d46b5cc3cdb
88eb87f67aefe33b394ba0eb9f50177b9feade449c5960a972a771bdde985f0f
56bab1697544e577a53b6e30f0c2a9e12a949565fe70e43f62893bc2ae11e2cf
31af353b8c7e7d376d2e6c761e753c264366cf2435954a9f46eeb2f99ed1033e
f5ec08868569fde84841699445ab8c9f95dbef253ec120838053f14badd0af5e
ea2d71af9790b0a058d0d166c52c2609a1a106053189c515b6059b5f18e9e48b
d42f53c75818af4aae281a0c3f760e2064385240 5d69134d03f6ba5c62efe316

KPMG Cyber Threat Intelligence Platform

Ursnif - Evolutionary Exploits of a Banking Trojan

Indicators of Compromise: Hashes
b4a95906cc39ee45ffaa914062843b9527ca3258ca56e88a97a75515ae5d1ade
a74e0504c5d39b686b89293d4221db4577079e6247af777d2f896524c8836aad
e999890ce5eb5b4565636501453O8ae837d940e38aec50d2f02670671d472b99
16323b3e56a0cbbba742b8d0af8519f53a78c13f9b3473352fcce2d28660cb37
6a9b7c289d7338760dd38d42a9e61d155ae906c14e80a1fed2ec62a4327a4f71
5b51bd2518ad4b9353898ed329f1b2b60f72142f90cd7e37ee42579ee1b645be
6c5338d84c208b37a4ec5e13baf6e1906bd9669e18006530bf541e1d466ba819
8e570e32acb99abfd0daf62cff13a09eb694ebfa633a365d224aefc6449f97de
1cdbf7c8a45b753bb5c2ea1c9fb2e53377d07a3c84eb29a1b15cdc140837f654
B94810947c33a0a0dcd79743a8db049b8e45e73ca25c9bfbf4bfed364715791b
C77ea4ad228ecad750fb7d4404adc06d7a28dbb6a5e0cf1448c694d692598f4f
dfdfd0a339fe03549b2475811b106866d035954e9bc002f20b0f69e0f98683 8f