Hive Pro

THREAT ADVISORY

SnatchCrypto campaign carried out by North Korean APT 38 subsidiary BlueNoroff

TA2022010

Threat Level RED

Publish Date – Jan 14, 2022

BlueNoroff, an advanced persistent threat (APT) group that's part of the larger Lazarus Group associated with North Korea, is behind a series of attacks against small and medium-sized companies that have led to serious cryptocurrency losses.

The campaign, dubbed SnatchCrypto, is aimed at various companies that, by the nature of their work, deal with cryptocurrencies and smart contracts, DeFi, Blockchain, and the FinTech industry. An elaborate social engineering attack is carried out by Attackers. Actors send these startup employees a full-featured phishing email having Windows backdoor with surveillance functions, disguised as a contract or another business file. If the file is opened on a device connected to the Internet, another macro-enabled document would be obtained to deploy malware.

The malware is exploiting the vulnerability CVE-2017-0199 which initially allowed automatic execution of a remote script linked to a weaponized document. This malware sends the target's general information and PowerShell agent to the attackers, creating a backdoor. From there, BlueNoroff deploys additional tools, including a keylogger and screenshot taker, to monitor victims. After weeks or months of tracking, the attackers find a prominent target and use the data they've collected to steal large amounts of cryptocurrency from them.

The TTPs used by **BlueNoroff** include:
T1192 - Spear phishing Link
T1059.005 - Visual Basic
T1059.001 - PowerShell
T1055.001 - Dynamic-link Library Injection
T1056.001 - Keylogging
T1113 - Screen Capture
T1132 - Data Encoding
T1027 - Obfuscated Files or Information
T1119 - Automated Collection
T1176 - Browser Extensions

Actor Detail

Name	Known as	Origin	Target Locations	Target sectors
Bluenoroff	NICKEL GLADSTONE, BeagleBoyz,, Stardust Chollima, CTG-6459 and APT 38	North Korea	Russia, Poland, Slovenia, Ukraine, the Czech Republic, China, India, US, Hong Kong, Singapore, the UAEIndonesia, the UK, Sweden, Germany, Bulgaria, Estonia, Malta, Portugal and Vietnam	cryptocurrencies and smart contracts, DeFi, blockchains, and FinTech industry

Hive Pro

THREAT ADVISORY

Vulnerability Detail

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2017-0199	Microsoft Office 2007 sp3, 2010 sp2, 2013 sp1, 2016, windows 7 sp1, server 2008 sp2, server 2008 r2 sp1, server 2012, vista sp2	cpe:2.3:a:microsoft:office:2007:sp3:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:2010:sp2:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:2013:sp1:*:*:*:*:*:*:*, cpe:2.3:a:microsoft:office:2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_7:*:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:*:sp2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:-:*:*:*:*:*:*:*:*,, cpe:2.3:o:microsoft:windows_vista:*:sp2:*:*:*:*:*:*:*	Microsoft Office and WordPad remote code execution	CWE-20

Indicators of Compromise(IoCs)

Type	Value
MD5	3812cdc4225182326b1425c9f3c2d50b, 4274e6dbc2b7aee4ef080d19fff47ce7, a3c61de3938e7599c0199d2778f7d417, 00a145e8f67a92b01ce4d85a0ed6bd77, 00a63a302dcaffc9f28826e9dba30e03, 02904e802b5dc2f85eec83e3c1948374, 033609f8672303feb70a4c0f80243349, 04deb35316ebe1789da042c8876c0622, 09bca3ddbc55f22577d2f3a7fda22d1c, 0a9b8ca2988208b876b74641c07f631e, 4bb579d59830579be9ead9f74a55001e, 849dd9e09cc2434ee7dbdbf9e1c408b2, 97e5c0fe8089da97665a22975e2c86de, bdc354506d6c018b52cb92a9d91f5f7c, d8e51f1b9f78785ed7449145b705b2e4, dd2d50d2f088ba65a3751e555e0dea71, ea9d8b81c9f85fd142639997187b447e, ec2b51dc1dc99165a0eb46b73c317e25, f1cfd14b030e6b5d75e777ace530dad9, ff28ec14ec926b9892c61b9bf154a910
Ipv4	118.70.116.154, 163.25.24.44 , 45.238.25.2

Hive Pro

THREAT ADVISORY

Type	Value
SHA-256	024ce4d9aabf0a25ca609d356c4a6254b0cdc1e57c93f50a4d2a907b01861e21, 02d8b12b641379001f3236bef47d91abf1d4f58a4e62a67202295521a6b601f5, 09b83a501b8f919fc4861735097dd50957f21e81209d362b4fa425bd3348a495, 156d33cd77b439e59220722069633d6ca60718bf71c271fee9e3105ba59a6e43, 1939d9fdcf831dc4cac001ba193669c75a336258bc99a1775471554229e4a69b, 19939221b42945f254c280e7029b02a397e9e3d78e200293bf3c8f2ec4400a5c, 1bd1853d2d1fdd6605b3295e09223a364e1dc160462fd9cb912d09c5ce919bd1, 1c9d1c2725ea0ef74a16d4d3e83b8e02d6e427266dc5ede660198165e865ddc4, 27f6c9a0765f8b44bac8edccfe852facb89396d7acb8d39d75b07d1e5bea6522, 290c2e4d0efbed23de0d41d1b821396f5f1003f6f123ee6160d6d5028d01b961
hostname	www.onlinedocpage.org, www.googlesheetpage.org, www.googledocpage.com, word.azureword.com, verify.googleauth.pro, upload.gdrives.best, up.digifincx.com, tokentrack.mrbasic.com, tokenhub.mefound.com, svr04.faqserv.com
Domain	youbicapital.cc venturelabo.co updatepool.online upcraft.io skandiafastigheter.cc sinovationventures.co sharedocs.xyz securedigitalmarkets.ca reit.live

Patch Link

https://msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0199

References

The BlueNoroff cryptocurrency hunt is still on - AlienVault - Open Threat Exchange
https://usa.kaspersky.com/about/press-releases/2022_bluenoroff-threat-actor-drains-cryptocurrency-startups-accounts
https://www.darkreading.com/attacks-breaches/bluenoroff-threat-group-targets-cryptocurrency-startups