侵入の痕跡（Indicators of Compromise, IoC

ファイル名（Description）	Hash	トレンドマイクロによる検出名
Exploit Html	bb1e9ce455898d6b4d31b2219ff4a5ca9908f7ea0d8046acf846bf839bce1e56	Trojan.HTML.CVE202140444.B
payload.cab	a20abef4eecea05b3f3ab64e9f448159e683cf82f1e87a37372c1cacb976052c	Trojan.Win32.CVE202140444.B
avatar.ps1	6f11be4822381543eb9dd99a9354575c96a50a5720ee38ee1c1b2ad323a03f04	Trojan.PS1.POWLOAD.TIAOELH
payload_TNICAYLA.exe_	f7c5f885f712adb553ee0de0d935869cc9c5627c01b15a614d748acb72b11c74	Trojan.Win32.FORMBOOK.PUSXYV
injector_ncrypt_decompressedByteArray.exe_	eab5dc8f37459f2f329afa63b1f8e8569ad229dc88497ab86e7c6a91be4d9264	Trojan.Win32.CRYPTINJECT.DV

Exploit chain IOCs:

- hxxp://0x6B[.]0254.0113.0244:8090/payload.cab
- hxxp://107[.]172.75.164:8090/microsoftonline.html
- hxxps://cdn[.]discordapp.com/attachments/889336010087989260/889336402121199686/avatar.jpg

URLs

- hxxp://www.code-nana.com/pjje/?t8LP2P=Mf6ydddwV/QU6mZ4nnZxMBdzDcAr2xsvfTgD82WAzYYrxOcjLRrG5mXLygKxYmvGqlzJAQ==&kPq8=K4Nh-6

- hxxp://www.rajuherbalandspicegarden.com/pjje/?t8LP2P=DItNRLklEPawWuNnsQXifEZmZKsLvkDXv3cKYhiC/0Bh3Q72JrrE/8woD25qq/vxSOxjNQ==&kPq8=K4Nh-6
- hxxp://www.swaplenders.com/pjje/?t8LP2P=TQtLDRoafbQM4/pEtdovke1/MPx0w24gCyByZx68z3lV5KTK6L4nUj2UtH2v2BgU+KkBhg==&kPq8=K4Nh-6
- hxxp://www.thechiropractor.vegas/pjje/?t8LP2P=rpNmzTsgN3WrlTJLsfA2BlL5A0hwTnOMjBBWuUAz4iRkWF3ty9m96ejMesY0+5JvVxns9g==&kPq8=K4Nh-6

TREND MICRO ™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com