OPORD - OVERCOOKED RISOTTO

Operations Order - Operation: OVERCOOKED RISOTTO

Commanding Officer: LtCol Shelly “AJAX” Jackson

501st Cyber Interdiction Battalion, JCOG (Joint Cyber Operations Group)

[REDACTED LOCATION], [REDACTED LOCATION]

SITUATION

Cyber Criminal operations cell RISOTTO GROUP is suspected to be active in Area of Operations (AO). 501st operators are tasked with intercepting RISOTTO GROUP, regaining control of a target webserver, and removing opposing force from target infrastructure.

BACKGROUND

INFINITY was a digital design firm active in the mid 2010s before the company’s dissolution in 2022. The INFINITY website was hosted at http://takedown[.]thm[.]local and included a description of the company and some of the company’s digital portfolio. The website was decommissioned and retired on March 22nd, 2022.

Reconnaissance operations report that the INFINITY website is now back online. Intel reports indicate the website is now serviceable as recently as ~24 hours prior to the release of this OPORD. Intelligence reports with high confidence that this is the work of RISOTTO GROUP, an active cyber criminal ring in this AO.

MISSION

- Identify indicators of compromise of the INFINITY webserver
- Regain positive control of the INFINITY webserver
- Prosecute and deny RISOTTO GROUP operators
- Produce proof of positive control of the target webserver (user.txt and root.txt)

RULES OF ENGAGEMENT

- All methods of cyber interdiction are authorized for this operation.
- Denial of Service is not authorized against the target webserver or any RISOTTO GROUP infrastructure in order to preserve post-operation intelligence gathering capabilities.

INTELLIGENCE BRIEF

RISOTTO GROUP’s capabilities include custom command & control (C2) infrastructure and custom malware development. RISOTTO GROUP’s primary development languages include Go, Nim, Rust, C, and C++. RISOTTO GROUP has also been observed deploying additional capabilities when required, including Living off the Land Binaries and Scripts (LOLBAS) and native languages like PowerShell. The latest C2 samples indicate RISOTTO GROUP is using a newer C2 framework known as NIMBLEWISP.

RISOTTO GROUP does not often encrypt their C2 communication channels and forsake stealth for speed. RISOTTO GROUP is known to deploy malware keying tactics to ensure target accountability during operations. Keying values include username, hostname, domain name, and/or domain joined status. RISOTTO GROUP’s motivations are primarily financial.

RISOTTO GROUP operators are not particularly skilled but follow pre-defined playbooks (AGGRESSOR) when conducting operations. AGGRESSOR TTPs include basic enumeration and exfiltration of files to the NIMBLEWISP teamserver.

RISOTTO GROUP SAMPLE INDICATORS OF COMPROMISE / MALWARE (IOCs)

The following malware samples are attributed to RISOTTO GROUP.

MALWARE COVER NAME	SAMPLE NAME / FILE TYPE	TTP	SHA256 HASH
HAYDAY	cannonball.exe	Data Exfiltration	bd98f01b81fa4b671568d31fdc047fab76a2b7ce91352a029f27ce7f15ad401b
SHINESPARK	pspsps.ps1	Initial Access	450a60c214b7bbe186938d20830aa6402cf013af17d6751f6fe7b106deb4021e
SYNTHWAVE	whoHas.vbs	Encryption for Impact	d8a928b2043db77e340b523547bf16cb4aa483f0645fe0a290ed1f20aab76257
CHEAPCOLOGNE	mstupdater.exe	Persistence	ee13f4a800cffe4ff2eaafd56da207b0e583fac54d663ca561870e1bc4eeaad6
MAGICSTACK	urllib32.dll	Lateral Movement	ce0b1888dde30a95e35f9bcf0d914b63764107f15fb57c5606e29b06f08874a1
GUNRUNNER	favicon.ico	Initial Access	80e19a10aca1fd48388735a8e2cfc8021724312e1899a1ed8829db9003c2b2dc
CHIVALROUSTOAD	srv.vbs	Persistence	707dd13b5b61ecb73179fe6a5455095f0976d364e129e95c8ad0a01983876ecb
GRIDLOCK	regsrv86.dll	Persistence	dbf8f09abe7ff34f4f54f3af8a539f3dba063396d51764554105ce100c443dd2
OPTOMETRIC	shutterbug.jpg	Initial Access	265d515fbe1e8e19da9adeabebb4e197e2739dad60d38511d5d23de4fbcf3970
VIGOROUSWEASLE	shutdown.dll	Persistence	4d4584683472d8ec1ccf0d46e62a9fc54998fda96e12fa8d6e615ee0b7f36096

COMMAND AND SIGNAL

The Commanding Officer of this operation is LtCol Shelly “AJAX” Jackson. This OPORD is active upon receipt.