RECENT BAZARLOADER USE IN RANSOMWARE CAMPAIGNS

Executive Summary

On September 28, 2020, security researchers openly shared recent observations associated with RYUK ransomware deployments. This information comes following recent news reporting of a potential RYUK ransomware incident affecting a large US healthcare entity. Recent ransomware campaigns leveraged phishing followed by deployment of malware associated with TRICKBOT actors.

Analysis

Security researchers suggest the RYUK ransomware has returned from a roughly four-month hiatus with threat activity observed the week of September 17, 2020. This recent threat activity leverages phishing to establish persistence with BAZARLOADER (AKA TEAM9) followed by the commercially-available Cobalt Strike BEACON malware and ultimately the deployment of RYUK ransomware. In recent RYUK-related intrusions, time from phishing email to RYUK deployment was around three days.

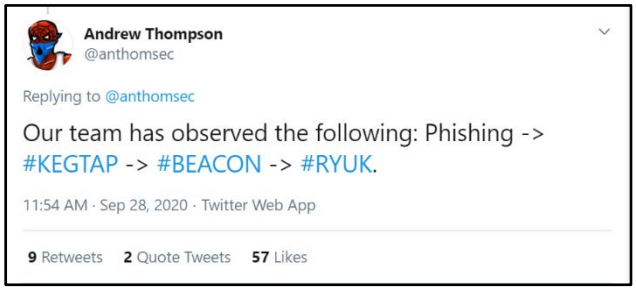

Figure 1. Tweet by Andrew Thompson sharing RYUK deployment observations on 28 September 2020. KEGTAP is also known as BAZARLOADER (AKA TEAM9).

The BAZARLOADER malware is a downloader that can establish persistence and execute additional payloads. The malware resolves its command and control (C2) servers using Emercoin DNS domains. According to BleepingComputer, the developers of the TRICKBOT are believed to be behind this backdoor due to code similarities, executable crypters, and its infrastructure.

The commercially-available Cobalt Strike BEACON malware is a backdoor commonly used for network penetration testing which supports several capabilities including injecting and executing arbitrary code, uploading and downloading files, and executing shell commands. Security researchers have recently identified active BEACON implants hosted on Amazon Web Services (AWS) and other infrastructure.

Finally, RYUK is a ransomware variant that uses a combination of public and symmetric-key cryptography to encrypt files on a host computer. The malware stops numerous services and kills a variety of processes that may interfere with the ransomware's functionality including anti-virus, database, and backup software.

The U.S. Department of the Treasury recently published an advisory for facilitating ransomware payments to sanctioned groups with the possibility of facing civil penalties for sanctions violations. While the RYUK operators are not currently listed, sanctioned ransomware groups include the developers of Cryptolocker, Iranian actors connected to SamSam ransomware, three North Korean hacking groups, and the Evil Corp cybercrime group.

Alert

HC3 is sending this alert related to recent RYUK ransomware campaigns. See below section titled "Patches, Mitigations & Workarounds" for associated Tactics, Techniques, and Procedures (TTPs) and Indicators of Compromise (IOCs) associated with BAZARLOADER, BEACON, and RYUK.

Patches, Mitigations & Workarounds:

Indicators of Compromise (IOCs) Associated with RYUK:

Indicator Type	Indicator
FileHash-MD5	c0202cf6aeab8437c638533d14563d35
FileHash-MD5	d348f536e214a47655af387408b4fca5
FileHash-MD5	958c594909933d4c82e93c22850194aa
FileHash-MD5	86c314bc2dc37ba84f7364acd5108c2b
FileHash-MD5	29340643ca2e6677c19e1d3bf351d654
FileHash-MD5	cb0c1248d3899358a375888bb4e8f3fe
FileHash-MD5	1354ac0d5be0c8d03f4e3aba78d2223e
FileHash-MD5	5ac0f050f93f86e69026faea1fbb4450
FileHash-MD5	32cbc69f85cc47d8e35dc20dfbda6948
FileHash-MD5	7a7b1300e8b5a10424e08958a6fc15c1
FileHash-MD5	40492c178079e65dfd5449bf899413b6
FileHash-MD5	dc83bab1982a5418b9ee448415317500
FileHash-MD5	29f99f63c076a29db46ada694a2201d3
FileHash-MD5	5ea06d5bffcf42780c1636cf9553d7eb

Indicators of Compromise (IOCs) Associated with Cobalt Strike BEACON:

Indicator Type	Indicator
IPv4	35.201.229[.]47:6666/RPEv
IPv4	35.201.229[.]47:6666/wICZ
IPv4	119.45.191[.]253:8080
URL	hxxp://ec2-18-222-171-22.us-east-2.compute.amazonaws[.]com/69wv

ATT&CK IDS Associated with BAZARLOADER:
T1055 - Process Injection, T1093 - Process Hollowing, T1192 - Spearphishing Link, T1186 - Process Doppelgänging, T1116 - Code Signing, T1204 - User Execution, T1106 - Native API, T1027 - Obfuscated Files or Information

Indicators of Compromise (IOCs) Associated with BAZARLOADER:

Indicator Type	Indicator
YARA	c238e928b89138125496c8fda96ac7d7868a4224
URL	https://allacestech.com/PreviewReport.DOC.exe
URL	https://www.ruths-brownies.com/PreviewReport.DOC.exe
URL	http://www.afboxmarket.com/CompanyReportList.exe
URL	http://invent-uae.com/Document_Preview.exe
URL	https://51.81.113.26/api/v88
URL	https://daralsaqi.com/PreviewReport.DOC.exe
FileHash-MD5	cdddcbc43905f8a1a12de465a8b4c5e5
FileHash-MD5	8f290a2eacfdcfea4f5ca054ae25bc62
FileHash-MD5	b533f8b604b2cc99ce938d8303994e43
FileHash-MD5	0e9f7f512a7eae62c091c7f0e2157d85

Indicator Type	Indicator
FileHash-MD5	267b23b206cde7086607e2c4471a97c4
FileHash-MD5	0708c3b1c48d71148cfd750e70511820
FileHash-MD5	df3db8d75d6c433c4c063d17f22e9b21
FileHash-MD5	3fe91dbbcf0962895f768da6e40853ee
FileHash-MD5	8b3215a899af33e3f6beb47a08787163
FileHash-MD5	3078b0b4b1dc48d62019d6ccca9cf098
FileHash-MD5	e16a92cccc3700196337c9ad43210f38
FileHash-MD5	9066f4c98967e27a1d32f01c47884785
FileHash-MD5	07d1c4952795e804b87c7c9d536dc547
FileHash-MD5	c25965d25b5ccdc2f401188f27972c22
Mutex	mn_185445
Mutex	ld_201127
domain	newgame.bazar
domain	thegame.bazar
domain	tallcareful.bazar
domain	realfish.bazar
domain	bestgame.bazar
domain	forgame.bazar
domain	portgame.bazar
domain	eventmoult.bazar
domain	coastdeny.bazar
domain	workrepair.bazar
FileHash-MD5	8aa10fc713d67d4ab34031a6f27024ba
FileHash-MD5	90a7b0c10eac98ff8d03823c19cd0add
FileHash-MD5	dfcf5342f034605cda27d08ce3706d0f
FileHash-MD5	b3b2333fa8195ad7003b6b3624ec7271
FileHash-MD5	a9952f532a7141910b2261394a52e6dc
FileHash-MD5	a5d0f9c549834d475a5faf9bc12974d7
FileHash-MD5	db9052ec56eed900354f4379d576e1b5
FileHash-MD5	2217d26aa15eec029c693c7ceedad0bf
FileHash-MD5	fd18f895de2806d7bfe6fcbd189e4bb9
domain	zirabuo.bazar
FileHash-MD5	8371ab023e4eb1f385926ad619d109b4
FileHash-MD5	c166858685bf0db063121601af5cf46e
FileHash-MD5	621ee1cc6f678123775d2dcf73250999
FileHash-MD5	11ca39d3b268610560b9f7595075bac0
FileHash-MD5	0677da0c04a2d64dcc1dcb80045a3d64
FileHash-MD5	6c6a2bfa5846fab374b2b97e65095ec9
FileHash-MD5	b2ad62cb18486b86aae7d53236ef9ed6
FileHash-MD5	3176c4a2755ae00f4fffe079608c7b25
FileHash-MD5	6dade484de2d790f287f4f248177f9d0
FileHash-MD5	7b5aa87ed32c53a8009fdfc738213d94

Indicator Type	Indicator
FileHash-MD5	ebb740d3759131a9914b9aea588a246d
FileHash-MD5	fa743c66268dea043d8068a5c96b4c43
FileHash-MD5	0374a343768b30771381a35ab7c0b854
FileHash-MD5	309ecc2d7ccaef74e5231b1671b73a8e
FileHash-MD5	fdf79b8921487469919bb95b940899e6
FileHash-MD5	c35cef0d8f236d510676004d41a7283f
FileHash-MD5	53329398c4a2a11a06016a9d45346216
FileHash-MD5	41ba0038d1edc5f2e2c001af2807cb10
FileHash-MD5	8aac391fe0aa02d7a8c3a5f34f35dd44
FileHash-MD5	c03f4ea15159222c609ededaddc57968
FileHash-MD5	a04c7e5f2c955caa18d90a4faee4f843
FileHash-MD5	a0ab22bc54244298d5928464fc7e62b1
FileHash-MD5	d40ea830655b4ed8264b238db1d7e0f4
FileHash-MD5	f990e4d13ae695e2f7a86c64919c53d7
FileHash-MD5	37aa5690094cb6d638d0f13851be4246
FileHash-MD5	9301564bdd572b0773f105287d8837c4
FileHash-MD5	0796f1c1ea0a142fc1eb7109a44c86cb
FileHash-MD5	3a4e4c14e837abe7cd571759149f855b
FileHash-MD5	01440a3c0c44b76462a96d67626720fe
URL	https://66.70.218.37/api/v92
URL	https://66.70.218.37/api/v90

References

https://twitter.com/fwosar/status/1309223351957815299
https://twitter.com/anthomsec/status/1310608927239933954
https://securityboulevard.com/2020/09/cobalt-strike-the-new-favorite-among-thieves/
https://twitter.com/d4rksystem/status/1311682291530444800
https://www.bleepingcomputer.com/news/security/bazarbackdoor-trickbot-gang-s-new-stealthy-network-hacking-malware/
https://www.vkremez.com/2020/04/lets-learn-trickbot-bazarbackdoor.html
https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/group-behind-trickbot-spreads-fileless-bazarbackdoor
https://blog.fox-it.com/2020/06/02/in-depth-analysis-of-the-new-team9-malware-family/
https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf