Cyber Intelligence Report

Date	2022-02-24
ID	TI20220224171002575
Source Type	Clear Web
Severity	High
Event Type	Early Warning

Descrizione

Alla luce della delicata situazione geopolitica causata dalla tensione russo-ucraina, vi sono evidenze della distribuzione di due nuovi malware denominati **HermeticWiper** e **Cyclops Blink** sfruttati attivamente contro le infrastrutture ucraine.

La portata dell'attacco potrebbe non essere limitata alle infrastrutture ucraine, la diffusione del malware Cyclops Blink è stata individuata anche verso organizzazioni nel territorio italiano.

Si raccomanda l'implementazione degli indicatori di compromissione individuati al fine di identificare la presenza di eventuali artefatti malevoli sui propri sistemi.

Analisi tecnica

Di seguito i dettagli dei malware identificati:

HermeticWiper
Malware di tipo "wiper" utilizzato contro le organizzazioni ucraine ed osservato dal team di Threat Intelligence di Symantec anche in Lettonia e Lituania. [1]
Questo wiper sfrutta dei drivers legittimi del software *EaseUS Partition Master* al fine di corrompere i dati presenti nel dispositivo compromesso e renderli irrecuperabili. [2]

Indicatori di Compromissione:

Type	Value
Hash	1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591
Hash	61b25d11392172e587d8da3045812a66c3385451
Hash	912342f1c840a42f6b74132f8a7c4ffe7d40fb77
Hash	3f4a16b29f2f0532b7ce3e7656799125
Hash	a952e288a1ead66490b3275a807f52e5
Hash	84ba0197920fd3e2b7dfa719fee09d2f
Hash	0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
Hash	231b3385ac17e41c5bb1b1fcb59599c4
Hash	095a1678021b034903c85dd5acb447ad
Hash	eb845b7a16ed82bd248e395d9852f467

Ulteriori dettagli sono disponibili in [1][2][3].

Cyclops Blink
Malware distribuito da parte del gruppo *Sandworm* (alias *Voodoo Bear*); questo threat actor viene associato da NCSC, CISA, ed FBI ad una unità militare speciale del GRU, a cui sono già state attribuite attività malevole in passato fra le quali:

- BlackEnergy
- NotPetya

Cyclops Blink viene considerato un malware sostitutivo di VPNFilter [4], e viene distribuito verso dispositivi di rete SOHO (Small Office/Home Office) esposti su Internet, in particolare sono stati individuati sample specifici

per dispositivi *Watchguard*, anche se è probabile che il malware sia compilabile per altre architetture e firmware [5].
Al fine di identificare e rimuovere Cyclops Bling dai dispositivi compromessi, *Watchguard* ha rilasciato delle linee guida ed un tool apposito.[8]

Indicatori di Compromissione:

Type	Value
IPv4	96.80.68.193
IPv4	93.51.177.66
IPv4	90.63.245.175
IPv4	81.4.177.118
IPv4	80.155.38.210
IPv4	80.153.75.103
IPv4	80.15.113.188
IPv4	78.134.89.167
IPv4	70.62.153.174
IPv4	50.255.126.65
IPv4	37.99.163.162
IPv4	37.71.147.186
IPv4	217.57.80.18
IPv4	212.202.147.10
IPv4	208.81.37.50
IPv4	185.82.169.99
IPv4	151.0.169.250
IPv4	109.192.30.125
IPv4	100.43.220.234
IPv4	212.234.179.113
IPv4	212.103.208.182
IPv4	188.152.254.170
IPv4	105.159.248.137
IPv4	24.199.247.222
IPv4	2.230.110.137
Hash	ff17ccd8c96059461710711fcc8372cfea5f0f9eb566ceb6ab709ea871190dc6
Hash	d01e2c2e8df92edeb8298c55211bc4b6
Hash	c59bc17659daca1b1ce65b6af077f86a648ad8a8
Hash	c082a9117294fa4880d75a2625cf80f63c8bb159b54a7151553969541ac35862
Hash	bbb76de7654337fb6c2e851d106cebc7
Hash	7d61c0dd0cd901221a9dff9df09bb90810754f10
Hash	50df5734dd0c6c5983c21278f119527f9fdf6ef1d7e808a29754ebc5253e9a86
Hash	4e69bbb61329ace36fbe62f9fb6ca49c37e2e5a5293545c44d155641934e39d1
Hash	438cd40caca70cafe5ca436b36ef7d3a6321e858
Hash	3f22c0aeb1eec4350868368ea1cc798c
Hash	3c9d46dc4e664e20f1a7256e14a33766
Hash	3adf9a59743bc5d8399f67cab5eb2daf28b9b863

Ulteriori dettagli sono disponibili in [5][6][7].

Spettro di impatto

Di seguito sono riportati i sistemi vulnerabili ad i malware HermeticWiper e Cyclops Blink:

HermeticWiper

- Dispositivi Windows

Cyclops Blink

- Cyclops Blink è un file Linux ELF malevolo compilato per architetture 32-bit PowerPC (big-endian), il suo target sono dispositivi SOHO (Small Office/Home Office) esposti su Internet ed in particolare Watchguard.

Processo di remediation

Il team di Yarix raccomanda di intraprendere le seguenti azioni:

- Implementare gli IoC presenti all'interno di questo report;
- Mantenere aggiornati i sistemi esposti sulla rete;
- Implementare l'autenticazione a più fattori sui servizi critici;
- Assicurarsi che le interfacce di gestione dei dispositivi di rete non siano esposte su Internet;
- Prestare la massima attenzione agli allegati provenienti da fonti sconosciute;

Riferimenti

[1] https://www.bleepingcomputer.com/news/security/new-data-wiping-malware-used-in-destructive-attacks-on-ukraine/
[2] https://csirt.gov.it/contenuti/ucraina-pubblicati-nuovi-importanti-ed-urgenti-ioc-al01-220224-csirt-ita
[3] https://twitter.com/ESETresearch/status/1496581903205511181?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1496581903205511181%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.reuters.com%2Ftechnology%2Fdestructive-malware-circulating-ukraine-has-hit-hundreds-computers-eset-2022-02-23%2F
[4] https://blog.talosintelligence.com/2018/05/VPNFilter.html
[5] https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
[6] https://csirt.gov.it/contenuti/cyclops-blink-nuovo-malware-distribuito-anche-sul-territorio-italiano-al02-220224-csirt-ita
[7] https://www.ncsc.gov.uk/files/Cyclops-Blink-Malware-Analysis-Report.pdf
[8] https://detection.watchguard.com/