De Malware a Ransomware

cronup.com/post/de-ataque-con-malware-a-incidente-de-ransomware

May 3, 2021

El Ransomware hoy en día, es una de las ciberamenazas más importantes a nivel mundial ya que no solo compromete los activos digitales sino que también la información sensible y privada de las empresas que son víctima, sin embargo, el Ransomware es el payload final y muchos de estos ataques provienen de una infección previa con Malware de distinto tipo como por ejemplo loaders, RAT o troyanos bancarios.

El listado La imagen a continuación, reúne las distintas familias de Malware que podrían derivar a un incidente de Ransomware, comprometiendo la red y la información corporativa.

A continuación, dejamos links de referencia que permiten relacionar cada una de estas amenazas e involucran además información como la descripción, IoCs, investigaciones, reportes, recursos, reglas de detección (Yara) y análisis de incidentes entre otros.

2.- Emotet -> Trickbot -> Ryuk

3.- Trickbot -> Ryuk

4.- Trickbot -> Conti

5.- Vatet -> PyXie -> Defray777 / RansomEXX

6.- IcedID -> Vatet -> PyXie -> Defray777 / RansomEXX

7.- IcedID -> Egregor

8.- IcedID -> REvil / Sodinokibi

https://thedfirreport.com/2021/03/29/sodinokibi-aka-revil-ransomware/ (29-03-2021)

9.- Ursnif -> Egregor

https://unit42.paloaltonetworks.com/egregor-ransomware-courses-of-action/ (08-12-2020)

10.- Qakbot -> Egregor

- https://www.bleepingcomputer.com/news/security/qbot-partners-with-egregor-ransomware-in-bot-fueled-attacks/ (20-11-2020)
- https://unit42.paloaltonetworks.com/egregor-ransomware-courses-of-action/ (08-12-2020)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.qakbot
- https://malpedia.caad.fkie.fraunhofer.de/details/win.egregor

11.- Qakbot -> ProLock

- https://www.bleepingcomputer.com/news/security/prolock-ransomware-teams-up-with-qakbot-trojan-for-network-access/ (14-05-2020)
- https://raw.githubusercontent.com/fboldewin/When-ransomware-hits-an-ATM-giant—The-Diebold-Nixdorf-case-dissected/main/When%20ransomware%20hits%20an%20ATM%20giant%20-%20The%20Diebold%20Nixdorf%20case%20dissected%20-%20Group-IB%20CyberCrimeCon2020.pdf
- https://malpedia.caad.fkie.fraunhofer.de/details/win.pwndlocker

12.- Qakbot -> MegaCortex

- https://success.trendmicro.com/solution/1122802-megacortex-ransomware-information (30-12-2019)
- https://cyware.com/news/qbot-trojan-a-quick-analysis-of-a-decade-old-banking-trojan-bd6d0efd (02-09-2020)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.megacortex

13.- Zloader -> Egregor

- https://malpedia.caad.fkie.fraunhofer.de/details/win.zloader
- https://malpedia.caad.fkie.fraunhofer.de/details/win.egregor
- https://twitter.com/likethecoins/status/1327309590736883712
- https://twitter.com/VK_Intel/status/1324377307109347329

14.- Zloader -> Ryuk

- https://lifars.com/wp-content/uploads/2020/10/The-Assassin-Squad-Zbot-and-RYUK-1.pdf (10-2020)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.zloader
- https://twitter.com/fffforward/status/1324281530026524672

15.- Zloader -> DarkSide

https://www.advanced-intel.com/post/from-dawn-to-silent-night-darkside-ransomware-initial-attack-vector-evolution (14-05-2021)

16.- SDBBot -> Clop

- https://www.zdnet.com/article/australian-government-warns-of-possible-ransomware-attacks-on-health-sector/ (13-11-2020)
- https://blog.fox-it.com/2020/11/16/ta505-a-brief-history-of-their-time (16-11-2020)
- https://www.cronup.com/post/threat-alert-grupo-ta505-reinicia-ataques-en-latinoam%C3%A9rica
- https://www.cyber.gov.au/acsc/view-all-content/alerts/sdbbot-targeting-health-sector
- https://malpedia.caad.fkie.fraunhofer.de/details/win.sdbbot
- https://malpedia.caad.fkie.fraunhofer.de/details/win.clop

17.- Dridex -> DoppelPaymer

- https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html (05-01-2021)
- https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/ (12-07-2019)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.doppelpaymer

18.- Dridex -> BitPaymer

- https://www.cert.ssi.gouv.fr/uploads/CERTFR-2020-CTI-008.pdf (17-07-2020)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.friedex

19.- Gootkit -> REvil / Sodinokibi

- https://www.bleepingcomputer.com/news/security/gootkit-malware-returns-to-life-alongside-revil-ransomware/ (30-11-2020)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.gootkit
- https://malpedia.caad.fkie.fraunhofer.de/details/win.revil

20.- Phorpiex -> Avaddon

- https://blog.checkpoint.com/2020/12/09/november-2020s-most-wanted-malware-notorious-phorpiex-botnet-returns-as-most-impactful-infection/ (09-12-2020)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.phorpiex
- https://malpedia.caad.fkie.fraunhofer.de/details/win.avaddon

21.- Phorpiex -> Nemty

- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/nemty-ransomware-trik-botnet (04-11-2019)
- https://www.lastline.com/labsblog/nemty-ransomware-scaling-up-apac-mailboxes-swarmed-dual-downloaders/ (18-02-2020)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.nemty

22.- BazarLoader / BazarBackdoor -> Ryuk

- https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/ (18-10-2020)
- https://storage.pardot.com/652283/16118467480sqebwq7/MSP_Security_Summit___John_Hammond_Huntress___Analyzing_Ryuk.pdf
- https://malpedia.caad.fkie.fraunhofer.de/details/win.bazarbackdoor

23.- BazarLoader / BazarBackdoor -> Conti

- https://www.cybereason.com/blog/cybereason-vs.-conti-ransomware (12-01-2021)
- https://www.crowdstrike.com/blog/wizard-spider-adversary-update/ (16-09-2020)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.conti

24.- DanaBot -> NonRansomware

- https://research.checkpoint.com/2019/danabot-demands-a-ransom-payment/ (20-06-2019)
- https://www.zdnet.com/article/danabot-banking-trojan-jumps-from-australia-to-german-targets/ (15-08-2019)

- https://malpedia.caad.fkie.fraunhofer.de/details/win.danabot

25.- SmokeLoader -> Crysis / Dharma

BONUS

A continuación, dos de los frameworks más utilizados por los actores de amenaza y grupos afiliados de Ransomware para la comunicación con los C&C (servidores de comando y control) y el movimiento lateral en la red víctima.

Estos frameworks corresponden a herramientas para ejercicios de tests de penetración, sin embargo, son muy utilizadas en el flujo de ataques a objetivos de alto valor.

1.- Cobalt Strike -> Multiple Ransomware Families

- https://thedfirreport.com/2020/10/18/ryuk-in-5-hours/ (18-09-2020)
- https://thedfirreport.com/2020/08/31/netwalker-ransomware-in-1-hour/ (31-08-2020)
- https://malpedia.caad.fkie.fraunhofer.de/details/win.cobalt_strike

2.- Empire -> Multiple Ransomware Families

NOTA: Un reporte similar a este se puede encontrar en https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/ donde se confirman algunas de las amenazas aquí señaladas.

La información de este artículo se ira actualizando en la medida que se tengan nuevos antecedentes.

Conoce al enemigo, mantente seguro.

Threat Intelligence Team
CronUp Ciberseguridad

Germán Fernández
Threat Researcher en CronUp Ciberseguridad
Líder Red Team & Cyber Threat Intelligence.