Introduction

Peter Manev -
QA/Trainer/Exec team - OISF
CSO - Stamus Networks
Twitter @pevma

Josh Stroschein -
Director of Training - OISF
Professor Dakota State University
Twitter @jstrosch
A Few Announcements

• Upcoming <Virtual> Trainings
  • Threat Hunting
  • Advanced Deployment and Configuration
  • Dates: TBD

• SuriCon 2021 is just around the corner!
  • Call for Talks is open
  • NEW - Call for Trainings
  • Poster session and scholarship
  • More information at suricon.net
Announcements Continued...

• OISF - the US non-profit organization with full-time developers dedicated to ensuring Suricata remains world-class

• Join our consortium - we offer several ways to support Suricata's development roadmap and growing community.
  • Details at https://oisf.net/ or contact us at info@oisf.net
And Finally, Our Next Webinar!

We’ve had a steady schedule of one a month and will continue that tempo!

• Follow our blogs and social media for official announcement
• Twitter: @suricata_ids
• https://suricata-ids.org/news/
Time to Enter the Danger Zone
Suricata is a high-performance network security monitoring engine with IDS, IPS capabilities.

- Open-source software - find it on Github
- Owned and developed by a community run 501c3 non-profit foundation - Open Information Security Foundation (OISF)
- Produces a high-level of situational awareness and detailed application layer transaction records from network traffic
What We Will Cover

Outputs used for hunting:

- Combining Suricata alert and protocol data correlation
- Malware traditional process of proliferation
- TTPs
- 2 hands-on real-world malware cases
  - CobaltS / Hancitor / FickerStealer / RATs
  - PurpleFoxEK / NuggetPhantom

OSS tools used in this webinar for visualizing the outputs:

- ELK/SELKS6
- Scirius CE
- EveBox
- Moloch
- CyberChef
What We Will Cover

Note on data used

- Public data
  - https://malware-traffic-analysis.net/2021/02/02/index.html
- Many thanks !!! to Brad @malware_traffic
- 1st case Hancitor, Cobalt Strike, Ficker Stealer, NetSupport RAT
  - Proliferation
  - What happened when
  - How
  - Combination of protocol data and alerts investigation
  - Hunt in noise
What We Will Cover

Note on data used

- Public data
  • [https://www.malware-traffic-analysis.net/2021/01/05/index.html](https://www.malware-traffic-analysis.net/2021/01/05/index.html)
- Many thanks !!! to Brad @malware_traffic
- 2nd case - PurpleFoxEK NuggetPhantom
  • Proliferation
  • Combination of protocol data and alerts investigation
  • Decompress/deobfuscate binaries/code used
How it can happen

- Phishing Mail / Weblink
  - MalDoc (exploit in)
    - 1st Malware in
      - Downloader/Stealer
      - Ransom
    - 2nd Malware in
      - CnC
      - Lateral
How it can happen

Phishing Mail / Weblink

MalDoc (exploit in)

1st Malware in

Downloader/Stealer

Ransom

2nd Malware in

CnC

Lateral

Nth Malware/tool in…
How it can happen

How it happens in general

Let’s start by having a look at an example of detonation of Hancitor

• https://app.any.run/tasks/534e3de9-18fd-4468-803d-c7a8b835fae0/
Let’s dive in
Conclusion

• Come out and play
  • Pcap:
    • https://www.malware-traffic-analysis.net/2021/01/05/index.html
    • https://malware-traffic-analysis.net/2021/02/02/index.html
  • Suricata forums/help/discussions: https://forum.suricata.io/
  • Suricata trainings/webinars: https://suricata-ids.org/training/
  • OISF: https://oisf.net/
  • SELKS 6: https://www.stamus-networks.com/selks-6
  • EveBox: https://evebox.org/
  • ELK 7 ready to use Dashboards/Vizs 450+
    https://github.com/StamusNetworks/KTS7
  • Grafana 7+ Dashboards/Vizs
    https://github.com/b4b857f6ee/selks_grafana_dashboard