GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

Cyber Nightmares: Shamoon & Red October

Fidelis XPS Advanced Threat Defense

Agenda

- Shamoon Demo
- Red October Demo
- Bonus - based on time
  - “njRAT” Demo
- References
- Contact Info

Shamoon Demo

- Last year, the Shamoon malware affected an Oil company in the Middle East and “wiped” around 30,000 computers in their network

- This section will focus on a live demonstration of how Shammon propagates, wipes system, how you can rebuild the file system structure, and how you can analyze this type of samples to find encoding keys, decode data in the carrier file, etc in order to generate a malware analysis report

  - Tools: VMware, Wireshark, Filemon, Regmon, WinHex, CryptTool, IDA, and OllyDbg

Red October Demo

- Red October was a cyberespionage malware discovered in October 2012 and uncovered in January 2013
- Red October was an advanced cyberespionage campaign intended to target diplomatic, governmental and scientific research organizations worldwide
- The attack was mainly performed through Spear Phishing attacks with weaponized carrier files (MS Word, and Excel docs) exploiting the “CVE-2009-3129”, “CVE-2010-3333”, “CVE-2012-0158” vulnerabilities and the “CVE-2011-3544” java vulnerability
- This section will focus on a live demonstration similar to the previous Shamoon one

References

- http://www.threatgeek.com/2012/11/fidelis-threat-advisory-1007.html
- http://threatgeek.typepad.com/files/fta-1007---shamoon-1.pdf
- http://www.threatgeek.com/2013/06/fidelis-threat-advisory-1009-njrat-uncovered.html
- http://threatgeek.typepad.com/files/fta-1009---njrat-uncovered-1.pdf
- http://www.securelist.com/en/blog/208193834/Shamoon_The_Wiper_further_details_Part_II
- http://www.securelist.com/en/blog/208193786/Shamoon_the_Wiper_Copycats_at_Work
- http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies
- http://www.securelist.com/en/analysis/204792265/Red_October_Detailed_Malware_Description_1_First_Stage_of_Attack

Contact Info

Harold Rodriguez

Email: harold.rodriguez@fidelissecurity.com

Company website: http://www.fidelissecurity.com/

Company blog website: http://www.threatgeek.com/

Youtube channel: http://www.youtube.com/user/FidSecSys