Threat Advisory

Fidelis Threat Advisory

Fidelis Cybersecurity's Threat Research team issues Fidelis Threat Advisory (FTA) documents in response to current security issues posing risks to enterprises everywhere.

Each Fidelis Threat Advisory (FTA) features an overview of the threat (e.g. timeline, threat vector(s), person(s) involved, malware behavior, and propagation techniques), risk assessment, and indicators and mitigation strategies.

FTA 1020 - Dissecting the Malware Involved in the INOCNATION Campaign - Last month, CrowdStrike published a blog on malware campaigns attributed to Sakula. We took a look at the malware specifically in the INOCNATION campaign to analyze what was new and different about the techniques used by the threat actor.

FTA 1019 - Ratcheting Down on JSocket: A PC and Android Threat - The JSocket Remote Access Tool, (RAT) has been used in global phishing attacks and its use has been implicated in a number of notable attacks. The malware was even found on the phone of Argentinian prosecutor Alberto Nisman, who was murdered in a high-profile case earlier this year. The goal of this paper is to provide some updates to our previous FTA on AlienSpy, the predecessor of JSocket, and to discuss its Android capabilities in detail.

View a list of IP address and hostnames observed as command-and-control

View a list of observed hashes of this malware

FTA 1018 - Looking at the Sky for a DarkComet - First created in 2008, DarkComet is an efficient, function-rich remote access tool (RAT) that has been leveraged against various targets. DarkComet's author immediately stopped offering the tool after its use against Syrian dissidents in 2012 by supporters of Syrian President Assad's regime, and even the latest version of the tool, a 5.4.1 Legacy that doesn't include a server builder, was discontinued.

Download FTA 1018 Appendix C

Download FTA 1018 Appendix D

FTA 1017 - Phishing in Plain Sight - Fidelis Cybersecurity analysis has identified unrelated cyber criminal activity leveraging the vulnerability cited in CVE-2014-4114, which was initially exploited by advanced persistent threat (APT) actors in October 2014.

Download the FTA 1017 Appendix

FTA 1016 - Pushdo It To Me One More Time - Once thought to be defunct, the resilient Pushdo has surfaced with infections observed in more than 50 countries, with a substantial infection rate located in the Asia-Pacific region

FTA 1015 - Ratting on AlienSpy - This report is a comprehensive description of AlienSpy, a remote access trojan (RAT) with significant capabilities that is currently being used in global phishing campaigns against consumers as well as enterprises.

Download IOCs in CSV format

FTA 1014 - Bots, Machines, and the Matrix - In the recent past, a Fidelis XPS user reported seeing detections of what appeared to be botnet-related malware. While that customer was protected, we at Fidelis Cybersecurity decided to take a closer look.

FTA 1013 - RAT in a jar: A phishing campaign using Unrecom - In the past two weeks, we have observed an increase in attack activity against the U.S. state and local government, technology, advisory services, health, and financial sectors through phishing emails with what appears to be a remote access trojan (RAT) known as Unrecom.

Download indicators in xlsx format

FTA 1012 - Gathering in the Middle East, Operation STTEAM - In the past week, we have observed an increase attack activity against the Oil & Gas industry in the Middle East by a group of threat actors using the following handle: “STTEAM”. The group has also been observed attacking and compromising state government websites in the same area.

FTA 1011 - Follow Up #1- Intruder File Report: Sneakernet Trojan - This threat advisory describes select malware functionality with some granularity, provides extended detail regarding the headquarters components C2 functionality, provides additional means of defensive detection of this malware and describes some interesting aspects of the malware as a whole.

FTA 1011 - New CDTO: A Sneakernet Trojan Solution - This threat advisory describes the functionality of the three malware files to include command inputs and the resulting behavior of the malware.

FTA 1010 - njRAT The Saga Continues - To this day, we continue to observe waves of blunt phishing attacks from compromised hosts in the Middle East, showing threat actors using multiple tools...
Download indicators in CSV format

FTA 1009 - “njRAT” Uncovered - In the past thirty days (30) an increase attack activity has been observed using the "njRAT" malware.

FTA 1008 - Darkseoul/Jokra - Similar to the Shamoon malware, Darkseoul/Jokra is a cyber-attack that infiltrated the South Korean broadcast and banking infrastructure and wiped out more than 35,000 systems.

FTA 1007 - Shamoon - Due to the recent spate of nation/state sponsored malware, Shamoon is another entry in this class that adds a destructive compontent in its targeted attack.

FTA 1006 - DNS There are a variety of techniques attackers can use to exploit DNS, but the presence of any of them indicates that an initial compromise has already occurred.

FTA 1005 - Reverse Tunnels - The two primary threats associated with reverse tunneling are network security policy violations and the potentially more serious threat of remote control of internal systems by a malicious outsider.

FTA 1004 - User-Agent Strings As the use of the UA string requires no protocol malformations and as there is no formal standard for the content or format of a UA string, its use as a C&C channel is difficult to detect and thus bypasses most security devices.

FTA 1003 - SSL Challenges - Advanced, purpose driven adversaries utilized fraudulent SSL certificates to attack prominent websites, calling to question the authenticity of SSL.

FTA 1002 - IPv6 - While IPv6 poses no threat itself, without the proper controls, it is a conduit for concealed threat activity on your network.IPv6 and associated tunneling protocols employed on IPv4 networks can be used to bypass firewalls and IPS devices that are not IPv6-and IP Tunnel aware.

FTA 1001 - The RSA Hack - An examination of the three-stage RSA attack (spear phishing, Poison Ivy reverse tunnel, and compromise of the SecureID system) and a discussion of Adobe Flash patch challenges.

Threat Advisory

Webinars

Brochures

Videos

White Papers

Industry Analyst Reports

Blog

Ebooks

Additional Resources:

Threat Advisory

Webinars

White Papers

Contact Us

Company

Partners

Resources

Sitemap Privacy Policy