The State of the ESILE/Lotus Blossom Campaign

Posted on: June 26, 2015 at 12:01 pm **Posted in:** Targeted Attacks
Author: MingYen Hsieh (Threat Researcher)

3 10

The Esile targeted attack campaign targeting various countries in the Southeast Asian region has been discussed in the media recently. This campaign – which was referred to by other researchers as Lotus Blossom – is believed to be the work of a nation-state actor due to the nature of the stolen information, which is more valuable to countries than either private companies or cybercriminals.

The Palo Alto Networks report discussed a targeted attack campaign that has been known to Trend Micro researchers for some time. We noted in our earlier targeted attack trends report that this particular campaign – which is known as the Elise/Esile campaign elsewhere – was already in use in 2012. Other researchers have noted that this campaign was active as early as 2007. This campaign and the tools used are familiar to Trend Micro, and we have developed appropriate solutions for this threat.

ESILE In A Nutshell

Our detection for the malware family used in the Elise campaign is BKDR_ESILE. Their arrival and behavior patterns are quite consistent: they arrive via a malicious Office document sent through spear-phishing. In many cases, these documents claim to be official government papers to make it more attractive for users to open these files.

If the document is opened, an exploit is used to execute a dropper (SetElise) on the system. This dropper is run and tries to establish persistence for the resident component (EliseDLL). It will first try to create a Windows service to start EliseDLL. Failing that, it will drop a loader (LoadElise) and then add an autorun registry entry to bring up the loader every time the system boots up.

The diagram below provides an overview of ESILE's architecture:

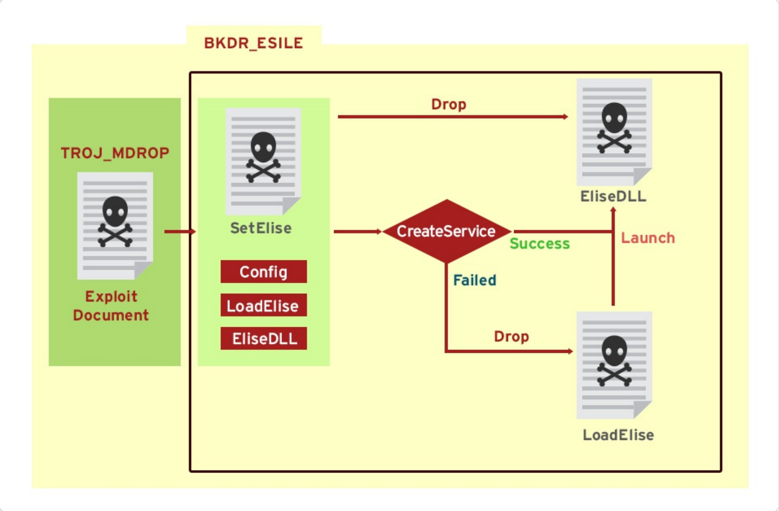


Figure 1. ESILE architecture

The initial command-and-control server information is embedded within the dropper. The string *DA76C979* or *DF72YR0V* is used as a marker for this information, which is located 40 bytes after the start of the tag. The file names of the loader and EliseDLL are also contained within the dropper.

One unique attribute of ESILE is that it (poorly) attempts to randomize the properties of the dropped files. Specifically, the created, last accessed, and last modified dates are all modified by the dropper. The dates used are randomly generated based on the following algorithm:

1. The year for these dates is set to 2007.

Featured Stories

- Microsoft Patches IE/Edge Zero-day Used in AdGholas Malvertising Campaign
- CVE-2016-6662 Advisory: Recent MySQL Code Execution/Privilege Escalation Zero-Day Vulnerability
- BkSoD by Ransomware: HDDCryptor Uses Commercial Tools to Encrypt Network Shares and Lock HDDs
- The French Dark Net Is Looking for Grammar Police
- Pokémon-themed Umbreon Linux Rootkit Hits x86, ARM Systems

Business Email Compromise

How can a sophisticated email scam cause more than $2.3 billion in damages to businesses around the world?
See the numbers behind BEC

Latest Ransomware Posts

- The Last Key on The Ring – Server Solutions to Ransomware
- Several Exploit Kits Now Deliver Cerber 4.0
- How Stampado Ransomware Analysis Led To Yara Improvements
- The Rise and Fall of Encryptor RaaS
- From RAR to JavaScript: Ransomware Figures in the Fluctuations of Email Attachments

Recent Posts

- Masque Attack Abuses iOS's Code Signing to Spoof Apps and Bypass Privacy Protection
- Control Flow Guard Improvements in Windows 10 Anniversary Update
- Patch Your Flash: Another Zero-Day Vulnerability Hits Adobe Flash
- BLACKGEAR Espionage Campaign Evolves, Adds Japan To Target List
- The Internet of Things Ecosystem is Broken. How Do We Fix It?

Ransomware 101

2. The day/hour/minute/second/millisecond fields are set using a random number generator (RNG). The seed for this RNG is set to the year of the dropper's release – i.e., a 2012 dropper will use 2012 as the seed.

Because of the fixed seed, the properties of the dropped files are not actually random, although at first glance they may appear to be. This may have been done to attempt to confuse security tools and researchers.

Another unusual property of ESILE malware is that some versions contain strings in their resources that, in effect, act as fingerprints that identify them as ESILE. These strings are:

- Elise Install Version 1.0
- Copyright (C) 2012

Command and Control

As is generally the case with backdoors, ESILE contacts a command-and-control server in order to receive commands from its attacker. *How* it does this is also a fingerprint of the campaign as well. It uses a URL based on the MAC address of the infected machine's network interface, as well as the current time.

For example: a victim's machine uses the MAC address 00-00-07-08-09-0A and attempts to connect to the C&C server at 2015-01-02 03:04:05. The URL used will be *http://{C&C server}:443/708090A/page_02030405.html*.

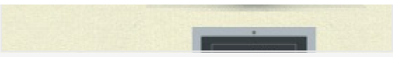
This distinctive pattern can be used to help spot and block ESILE-related endpoints on an organization's network.

Trend Micro Solutions and Best Practices

A variety of Trend Micro solutions are available to help protect users against this threat. Products with the ATSE (Advanced Threats Scan Engine), such as Deep Discovery, have heuristic rules which are capable of detecting attacks delivered via malicious attachments. These are detected as HEUR_OLEXP.X and EXPL_MSCOMCTL. Endpoint products can also detect the malicious attachments as TROJ_MDROP variants; the detection for the various ESILE components falls under the BKDR_ESILE family.

Trend Micro™ Custom Defense™ solutions can protect organizations from this type of attack. They provide in-depth contextual analysis and insight that help IT administrators properly identify suspicious behavior in the network, such as the access to the servers in this attack.

Tags: APT elise esile lotus blossom Targeted Attack



This infographic shows how ransomware has evolved, how big the problem has become, and ways to avoid being a ransomware victim.
Check the infographic

Popular Posts

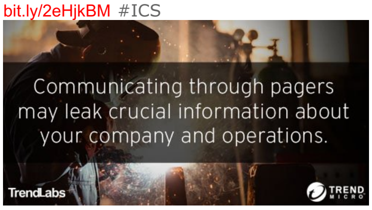
- DressCode and its Potential Impact for Enterprises
- Hacking Team Flash Zero-Day Integrated Into Exploit Kits
- Several Exploit Kits Now Deliver Cerber 4.0
- A Look at the BIND Vulnerability: CVE-2016-2776
- FastPOS Updates in Time for the Retail Sale Season

Latest Tweets

New post: Masque Attack Abuses iOS's Code Signing to Spoof Apps and Bypass Privacy Protection bit.ly/2f8pJCd @TrendMicro
about 2 hours ago

Massive DDoS attack resulting from Mirai-infected #IoT devices is a wake-up call to secure the IoT ecosystem.... twitter.com/i/web/status/7…
about 3 hours ago

Who still uses #pagers?!? You'd be surprised. Read our research here: bit.ly/2eHjkBM #ICS


Communicating through pagers may leak crucial information about your company and operations.
TrendLabs
TREND MICRO

about 9 hours ago

Stay Updated

Email Subscription

Your email here

HOME AND HOME OFFICE | FOR BUSINESS | SECURITY INTELLIGENCE | ABOUT TREND MICRO

Asia Pacific Region (APAC): Australia / New Zealand, 中国, 日本, 대한민국 , 台灣 Latin America Region (LAR): Brasil, México North America Region (NABU): United States, Canada
Europe, Middle East, & Africa Region (EMEA): France, Deutschland / Österreich / Schweiz, Italia, Россия, España, United Kingdom / Ireland

Privacy Statement Legal Policies