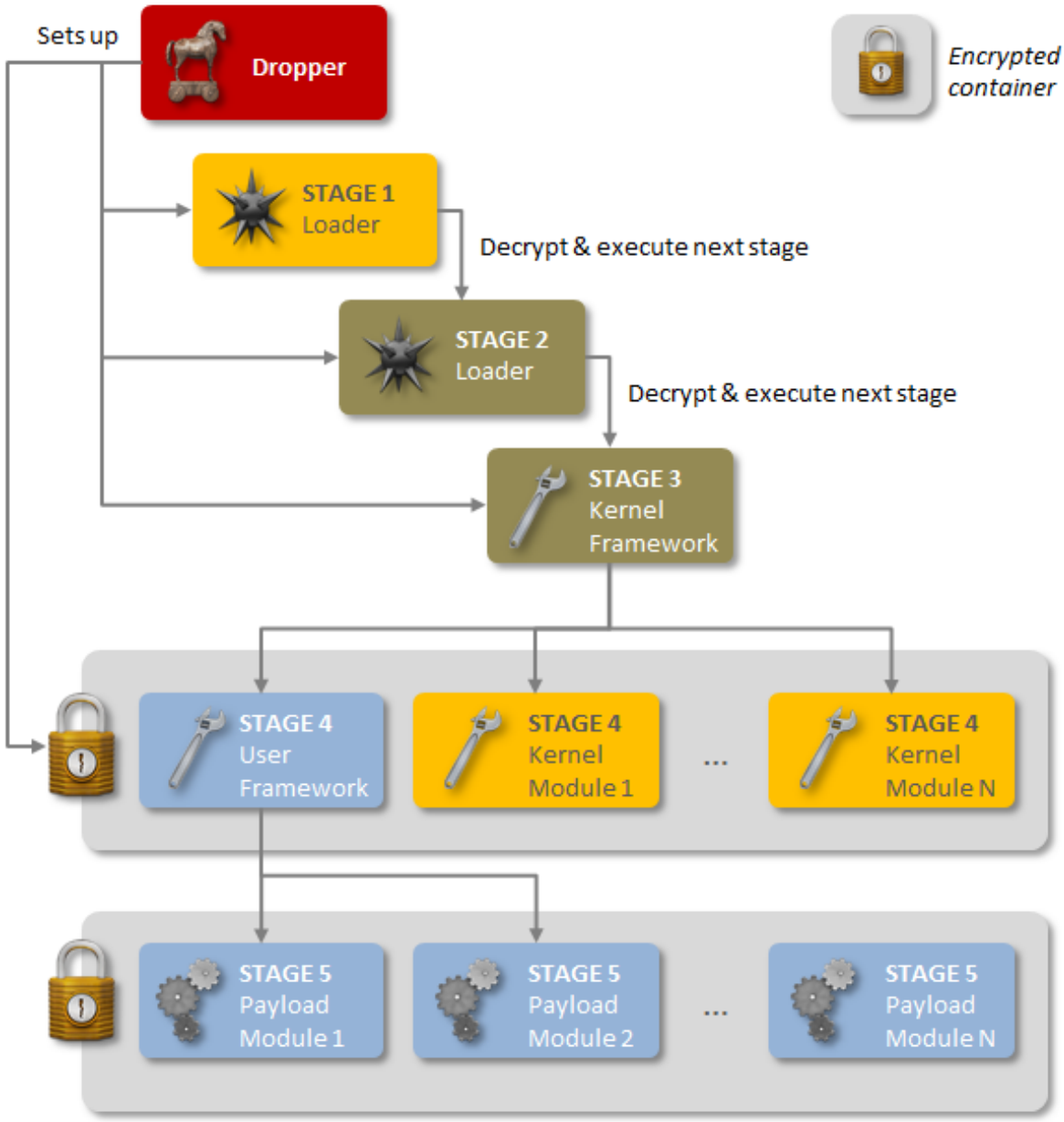
Security Now! #483 - 11-25-14

Let's Encrypt

Link Tracking Warning!
This document was first authored in Google Docs, then Downloaded as a PDF. So, Google has thoughtfully (ha!) added "tracking" redirections to all of the links here. (I have no idea why, but that's Google.) If that bothers you, simply copy the text of the link into your browser's URL field.

This week on Security Now!

- "Regin" (region), a new NationState-based **very** advanced persistent threat (VAPT).
- Let's Encrypt



Security News:

TOR may not be so anonymous after all...

- http://thestack.com/chakravarty-tor-traffic-analysis-141114
- A distressingly large percentage of TOR user IP addresses can be determined.
- Full coverage next week...

"Regin"

- "Registry" - "Install"
- Overview
- http://www.symantec.com/connect/blogs/regin-top-tier-espionage-tool-enables-stealthy-surveillance
- http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/regin-analysis.pdf
- Symantec's analysis begins with:
  In the world of malware threats, only a few rare examples can truly be considered groundbreaking and almost peerless. What we have seen in Regin is just such a class of malware.

  Regin is an extremely complex piece of software that can be customized with a wide range of different capabilities which can be deployed depending on the target. It is built on a framework that is designed to sustain long-term intelligence-gathering operations by remaining under the radar. It goes to extraordinary lengths to conceal itself and its activities on compromised computers. Its stealth combines many of the most advanced techniques that we have ever seen in use.

  The main purpose of Regin is intelligence gathering and it has been implicated in data collection operations against government organizations, infrastructure operators, businesses, academics, and private individuals. The level of sophistication and complexity of Regin suggests that the development of this threat could have taken well-resourced teams of developers many months or years to develop and maintain.

  Regin is a multi-staged, modular threat, meaning that it has a number of components, each depending on others, to perform attack operations. This modular approach gives flexibility to the threat operators as they can load custom features tailored to individual targets when required. Some custom payloads are very advanced and exhibit a high degree of expertise in specialist sectors. The modular design also makes analysis of the threat difficult, as all components must be available in order to fully understand it.

An (English-speaking) NationState Actor:

- Little question that this is the project of major nation-state.
- The nature of the malware's capabilities lead researchers to strongly suspect a nationstate sponsor/developer.
- For example just over one quarter of the detections have been on the communications backbone of telecom companies, and the installations' deployed modules are designed to gain access to the calls being routed through the telecom's infrastructure. This is not "hobby" malware.

- 2008 - 2011 ... then all use stopped until it reemerged in 2013...
- Targets include private companies, government entities and research institutes.
- Almost half of all infections targeted private individuals and small businesses.

Two Distinct Versions:

- V1.0 in use from at least 2008 through 2011.
- Appears to have been abruptly withdrawn from circulation and actively removed from infected target machines in 2011.
- v1.0 samples "left behind" were likely cutoff from communications or unable to be withdrawn.
- V2.0 in use from 2013 on, though possibly earlier.
- v2.0 has only been found in 64-bit form.

Architecture:

- 6-stage structure.
- Only the "dropper" / initial loader is visible on the machine. Everything else is stored in encrypted form, using a custom variant of the RC5 (a nice choice since it's a fast & simple, highly parameterized block cipher.)
- The initial dropper file has never been found/discovered.
- Stored as encrypted blobs in non-standard places, such as the registry, extended attributes, or raw sectors at the end of the disk.
- An OS within an OS... exporting a large specialized set of "framework functions" for use by other Regin modules.
    - Compression & decompression
    - Encryption & decryption
    - EVFS (encrypted virtual file system) handling
    - Container management
    - Log management
    - Loader
    - Network Operations
    - TCP command-and-control (C&C)
    - UDP C&C
    - C&C Processor

Injection Vector?:

- Varies among target and no reproducible vector has been found.
- One computer's log files showed that Regin got onto the machine through a Yahoo! Instant Messenger exploit.

Payloads:

- Completely modular with dozens of individual payloads... some are VERY advanced and highly targeted to specific entities... and evidencing a high degree of specialization in very specific industry sectors.
- Standard Capabilities include:

- Rootkit:
- The Stage 2 kernel driver hides running instances of Stage 1... removing all running code artifacts.

Modules for:

- Sniffing low-level network traffic
- Exfiltrating data through various channels (TCP, UDP, ICMP, HTTP)
- Gathering computer information
- Stealing passwords
- Gathering process and memory information
- Crawling through the file system
- Low level forensics capabilities (for example, retrieving files that were deleted)
- UI manipulation (remote mouse point & click activities, capturing screenshots, etc.)

Highly specific and advanced payloads, such as:

- Microsoft IIS server web traffic monitoring
- Sniff and gather administration traffic of cellular telephone base station controllers.
- Parse mail from Exchange mail databases.

Stealth:

- A great deal of work has been invested in having the malware keep itself hidden.
- It has several "stealth" features. These include:
    - Anti-forensics capabilities,
    - A custom-built encrypted virtual file system (EVFS),
    - Alternative encryption in the form of a variant of RC5, which isn't commonly used.
    - Regin uses multiple sophisticated means to covertly communicate with the attacker including via ICMP/ping, embedding commands in HTTP cookies, and custom TCP and UDP protocols.
- Exfiltrated data is often never written to disk but it retained in RAM, sent, and released.
- ICMP: Payload information can be encoded and embedded in lieu of legitimate ICMP/ping data.
- CRC checks use the seed '31337'.
- UDP: Raw UDP payload
- TCP: Raw TCP payload
- HTTP: Payload information can be encoded and embedded within cookie data under the names SESSID, SMSWAP, TW, WINKER, TIMESET, LASTVISIT, AST.NET_SessionId, PHPSESSID, or phpAds_d. This information can be combined with another cookie for validation under the names USERIDTK, UID, GRID, UID=PREF=ID, TM, __utma, LM, TMARK, VERSION, or CURRENT

Conclusions:

Regin is a highly-complex threat which has been used in systematic data collection or intelligence gathering campaigns.
The development and operation of this malware would have required a significant investment

of time and resources, indicating that a nation state is responsible.
Its design makes it highly suited for persistent, long term surveillance operations against targets.
The discovery of Regin highlights how significant investments continue to be made into the development of tools for use in intelligence gathering. Symantec believes that many components of Regin remain undiscovered and additional functionality and versions may exist. Additional analysis continues and Symantec will post any updates on future discoveries

Errata:

From: "Peter" <pete@petermcdonald.co.uk>
Subject: Possible Errata 481

I think you made a mistake when describing the S-Channel issue. You mentioned that sites running Apache and Nginx would be safe however surely this is not correct if they are running on windows.

Granted if they are using Apache or Nginx on Linux they would be safe.

Miscellany:

- Edward Snowden: CitizenFour

- Utah lawmaker wants to shut off NSA’s water supply for good
- http://arstechnica.com/tech-policy/2014/11/utah-lawmaker-wants-to-shut-off-nsas-water-supply-for-good/

SpinRite:

Andreas Gogstad
Location: Sandefjord, Norway
Subject: Spinrite success and question
Date: 24 Nov 2014 02:20:18

A user came in with a totally unreadable hard drive on a private PC. I took the opportunity to purchase SpinRite as payment for the recovery job after hearing about it many times on your podcast. I ran a level 2 scan despite warnings about an "invalid partition for drive size", since there wasn't much else to do and an LBA setting wasn't an option in the BIOS. I was then able to mount the drive on a Linux machine, which I did in Read Only mode and safety, and recover the photos she needed for her building permit application.

Could you explain the partition error message, and what the best solution in those cases would be?

Let's Encrypt

EFF, Mozilla, Cisco, Akamai, IdenTrust and the Uiversity of Michigan.

ACME Protocol. (JSON-over-HTTPS)

New independent entity will be creating a new Certificate Authority.

Using a new technology to prove domain ownership and automate fundamental certificate operations, this new CA will issue and manage FREE certificates for anybody who wants them.

The three certificate authentication levels:

- DV - Domain Validation.
- OV - Organization Validation.
- EV - Extended Validation.

Current System is entirely manual:

- Generate a CSR on the server.
    - Server holds the private key.
    - Places the Public key, along with other attributes such as Organization name, location, etc. into a binary blob CSR.
- Copy & Paste a CSR text blob into a CA's web page.
- CA performs whatever level of verification is needed
- CA sends the signed certificate back to the admin as an eMail attachment or user downloads from CA's website.
- User installs the certificate into their server.

Main Operations:

- Key pair authorization
- Certificate Issuance
- Certificate Revocation

Dialog:

- User / Client: I want to work with you to get a certificate for "example.com"
- Server: Here's a:
    - SessionID
    - Nonce
    - A list of ways to prove (challenges) your domain ownership/control
- User / Client: Here's...
    - Your SessionID back
    - My public key which I'll be using to prove I'm me for all future work with you on this domain name.
    - Your Nonce back
    - My signature of your Nonce

- My response(s) to one or more of your domain ownership/control challenges.

Challenges:

- Simple HTTPS:
  - CA specifies a page name and data to be placed online.
  - .well-known/acme-challenge/{path} (server provides the path) and data

- DVSNI
  - Domain Validation using Server Name Indication.
  - User's server generates a self-signed certificate with several fields in the "Subject Alternative Name" field.
  - actual domain under control
  - <hex(SHA256(hash of concatenation of nonces))>.acme.invalid

To revoke, the client simply uses its associated private key to sign a revocation request.

URL used with a future GET request to obtain another similar cert.

Recovery Token
Once ACME has been used the bar is raised.