DGA & Machine Learning (After NGIPS)

Johnny Yum / Solution Architect
Trend Micro TippingPoint
Johnny_yum@trendmicro.com
What is this?

Rig
Fiesta
Neutrino
Sweet Orange
Sundown
Nuclear
Magnitude
Angler
NextGen Exploit Kits

Angler-exploit-kit-hosting URLs were the most accessed in 2015. SweetOrange, Hanjuan, Fiesta, and Sundown exploit kits were rarely updated in 2015.
Angler EK

- Features
  - Encryption URL
  - DH Algorithm for C2 Server
  - Detects antivirus/hypervisor
  - Fireless infection
  - Uses zero-day vulnerability
  - Payload(CryptoWall, TeslaCrypt, Locky)

Obfuscation: 2567111413....

Order of letters: 2567111413.....
Ciphertext: Bwmcww.oyub.da.
Plaintext: www.badbuy.com
How Angler EK works?

- Compromised website
- Redirect
  - Malvertising
  - DNS shadowing
  - HTTP 302 cushioning
  - DGA
- Landing page
  - Scan/Exploit/Drop payload (Ransomware, ClickFraud, Keylogger, botnet etc)
  - Highly obfuscated script based content
DGA used in malware

Conficker  CryptoLocker
Simda      Dyre    BankPatch
Expiro     CryptoWall
Domain Generation Algorithms (DGAs)

- Domain Generation Algorithms
  - Used by modern malware to communicate with command and control (CnC) hosts
  - C&C hosts constantly change domain names to avoid blacklisting
  - Removes static domains names from downloaded malware to avoid detection
  - Too many possible domain names to sinkhole
DGA Sample

\^[a-z][a-f0-9]{33}\.(TLDs)\$

- Catches all Dyre domains
- No false positives
DGA FP Test

- Dyre – 0 False Positives (Alexa Top 1M)
- Bankpatch – 3 FP in Top 1M
- Expiro – 58 FP in Top 1M
- Generic (Linguistic) Detection – 42 in Top 1M
- 17 More in top 85M
- Equivalent to a needle in a haystack
How Angler EK works?

- Compromised website
- Redirect
  - Malvertising
  - DNS shadowing
  - HTTP 302 cushioning
  - DGA
- Landing page
  - Scan/Exploit/Drop payload (Ransomware, ClickFraud, Keylogger, botnet etc)
  - Highly obfuscated script based content
"...And who was leaning against the author of this behaviour; and so anxious for; it is impossible for to

to supply to her drawing-table as soon as she spoke,-- her

Her pleasure in seeing him. She instantly wrote Sir John against ever naming Mr. Willoughby, that will tempt YOU, Miss Marianne. "A dance!" cried Marianne.

I had no scruple of turning her eyes turned towards it, Marianne calmly said, "There, exactly there,"--pointing with one hand, "on that project

"Her heart was not honourable and flattering to me?"

Long letters from town, and is not written so well worth having as yours. And I hope not that. I might not come, for

"Mrs. Palmer's dressing-room. When there, at her request, Marianne engaged never to be long together; and if I

Jennings, "we know the summer will pass happily away. I mean to say--your friends are all lost on me. "I so."

Their were
Angler Detection

Machine Learning’s Bread and Butter
Machine Learning

• Implements new technology in TippingPoint IPS engine to use statistical data models to detect highly obfuscated script-based content
• Exploit-kits
• Obfuscated script (JS/VB)
• Malicious files (PDF, Flash, Pes, etc)
• 3 FPs on top 100k web sites from Alexa
How ML works?
Breach Protection System (BPS)

Intelligence on NG Threat
- EKs
- DGA
- Machine learning filter

Actionable Threat Defense

Visibility (IOA/IOC)

Operation Simplicity

Digital Vaccine
- Weekly Zero-day Vulnerability update (No CVE yet)
- Network Virtual Patch with Nexpose/Nessus/Qualys
  Lower latency

Advanced Threat Protection
- Custom Sandbox with live simulation
- Lateral movement
- Multiple Protocols

ThreatDV
THANK YOU

Johnny Yum
Trendmicro
+65 9631 3249
Johnny_yum@trendmicro.com