Are Legacy Malware Callbacks Clouding Your Security Operations Team

Jens Christian Høy Monrad
Global Intelligence Liaison / Analyst
FireEye iSIGHT Intelligence
@jenchm
We typically associate these types of malware and compromises as commodity, crimeware and legacy malware which is unsophisticated, only capable of sending spam, stealing social media logins, performing Bitcoin mining and in general considered, low hanging fruit, which does not require a lot of attention.

Reality is that it is a compromise that must be addressed
Defining Legacy Malware & Beaconing

- Abandoned Malware or Infrastructure
- Arrests of Creator(s) / Operator(s)
- Infrastructure Takedowns
SO WHY TALK ABOUT LEGACY MALWARE?
Expanding Attack Surface Area

- Windows
- Apple
- Internet 1.0
- Internet 2.0
- IOT

# OF THREAT ACTORS vs. ATTACK SURFACE
Ransomware Detections in EMEA

Ransomware detections in FireEye customers across EMEA 2015 till First Quarter of 2016
Ransomware Detections: GCC

- Bahrain
- Kuwait
- Oman
- Qatar
- Saudi Arabia
- United Arab Emirates

Percentages and timeline from 2015-01 to 2016-03.
We have to do more with less

* Survey by IDG Research on security automation: info.cgsi.com/idg-survey/
3 MALWARE CASE STORIES
Palevo & Mariposa

Believed to have infected 12M+ computers worldwide, including several Fortune 1000 Companies and Major Banks.

Managed to steal sensitive data (credentials, financial records, credit cards) from more than 800,000 users worldwide.

On December 2009, a joint operation took down the infrastructure and led to arrests of 3 individuals in Spain.
Ramnit

Infected more than 3 million computers worldwide. Evolved to steal credentials and other sensitive information.

5+ Years in operation, being a major criminal enterprise, defrauding a large number of victims.

Taken down in late February 2015 in a joint effort between Europol and multiple security and technology companies.
Cutwail & Pushdo

- Infected more than 2 million computers worldwide. Compromised computers become part of the spam-botnet via infections from the Trojan Pushdo.
- Spammers can rent an instance of the botnet for a fee and use in their own campaigns (in 2009 it was estimated that the network was responsible for almost 50% of all spam worldwide).
- In August 2010 an attempt to take down the botnet was performed and 20 out of the 30 C2 Servers were successfully taken offline.
2015 Observations
How Data Was Collected

- Buying expired & unused C2 domains
- Working with registrars on active C2 domains
- Monitor Incoming Connections – write signatures to match C2 strings
- Events stored with metadata (Organization Names, ASN etc.)
- Data sanitized before storing (i.e., no sensitive data transmitted)
Beaconing Observations: By Region

- Number of Organizations Observed in 2015

- **EMEA**: 22048
- **APAC**: 4406
- **AMERICAS**: 14259
Beaconing Observations: Total

- Number of Organizations Observed in 2015

- Americas: 35%
- APAC: 11%
- EMEA: 54%
- Anonymous Proxy: 0%
- Satellite Provider: 0%
- N/A: 0%

(Chart showing distribution of beaconing observations by region and category)
Beaconing Observations: GCC

- Number of Organizations Observed in 2015
  - United Arab Emirates: 34%
  - Saudi Arabia: 41%
  - Kuwait: 13%
  - Bahrain: 9%
  - Oman: 3%
Beaconing Observations: Industries

- Two Nuclear Power Plants
- Multiple state owned and private oil and natural gas companies
- A state-owned electric utilities company, supplying more than 50% of the total power in one country.
- Multiple Commercial Airlines
- A Nuclear facility which produces and enriches UF6 for Nuclear fuel.
- Multiple Nuclear Research Institutes
- Multiple Hospitals
- A National Air Force
- A Nuclear facility which produces and enriches UF6 for Nuclear fuel.
Risk Scenarios
Risk Scenario #1 – Prioritization of Alerts
Risk Scenario #2 – Disruption in ICS
Risk Scenario #3 – Attackers Regaining Control
Why Focus On Legacy Malware Callbacks?

- **Identify** - Develop the understanding to manage cyber security risk to systems, assets, data and capabilities
- **Protect** - Develop and implement safeguards to ensure delivery of services
- **Detect** - Develop and implement systems to identify the occurrence of a cyber security event
- **Respond** - Carry out actions to take once a cyber security event is underway
- **Recover** - Carry out activities to restore any capabilities or services impaired due to a cyber security event
COORDINATION STRATEGY FRAMEWORK
ADAPTIVE DEFENSE – A CAPABILITY MATURITY MODEL FRAMEWORK BY FIREEYE & EUROPOL

- IDENTIFY
- DETECT & RESPONSE
- THREAT VISIBILITY
- STRATEGIC INTELLIGENCE
- PLAN DEVELOPMENT
Cybersecurity is an Enterprise-wide Risk Management Issue

- What is acceptable risk?
- Where are your most important assets?
- How are they protected?
- What is the potential business impact of a breach?

- Time to detect if permeated?
- Time to contain once identified?
- What do your know about the attackers?
- What are the most effective actions?

- What is your remediation plan?
- What can you learn from this experience?
- What steps will improve your overall risk posture?
Next week you should:

- Start defining a plan, containing “Before, During and After” Scenarios

In the first three months following this presentation you should:

- Identify and Remediate Legacy Malware Compromises

Within six months you should:

- Have a measureable Security Operations Team, who focus on what is most critical for the business
Thank You