FireEye iSIGHT Intelligence

Robert Żelazo – Regional Director, Eastern Europe, FireEye

Prague, Sep 14, 2016
Some false things you may have heard around…

- “APT is just Advanced Malware, and you need Advanced Malware Protection”

- “Stop trying to Detect when you can Prevent”

- “Our APT solution offers Remediation”
The real problem is the hacker, not the malware

IT’S A “WHO,” NOT A “WHAT”
THERE’S A HUMAN AT A KEYBOARD
HIGHLY TAILORED AND CUSTOMIZED ATTACKS
TARGETED SPECIFICALLY AT YOU

THEY ARE PROFESSIONAL, ORGANIZED AND WELL FUNDED
NATION-STATE SPONSORED
ESCALATE SOPHISTICATION OF TACTICS AS NEEDED
RELENTLESSLY FOCUSED ON THEIR OBJECTIVE

IF YOU KICK THEM OUT THEY WILL RETURN
THEY HAVE SPECIFIC OBJECTIVES
THEIR GOAL IS LONG-TERM OCCUPATION
PERSISTENCE TOOLS ENSURE ONGOING ACCESS

The real problem is the hacker, not the malware
What happens after Malware?

- Expand Access and obtain valid credentials
  - Credentials stolen by keyboard logging
  - Credentials stolen by network sniffing
  - Encrypted Credentials stolen from disk and brute forced

- Strengthen foothold
  - Lateral movement using OS Tools
  - Further internal reconnaissance
  - Non malware based backdoors
  - Multiple backdoor fail-safes
APT29 – ONE OF THE MOST ADVANCED CYBERGROUPS
Russian Threat Groups

- FireEye monitors various Russian threat groups – for example:
  - APT28
  - APT29

- The groups frequently design innovative ways to cover their tracks

- APT29 has been particularly active throughout 2015
  - new downloaders, payloads, and targets
**APT29: Sponsored by the Russian Gov**

- Probable Russian threat actor supporting nation state missions
  - Espionage versus strategic European-related targets
  - Interest in Russia-Ukraine issues
  - Work hours align with the UTC +3 time zone (Moscow, St. Petersburg)
  - Operations ceased on Russian holidays

- Disciplined focus on operational security
  - Almost exclusive use of compromised servers, legitimate services, and similar
  - Anti forensics

- Aggressive and advanced skills
  - Targeting both intelligence targets and defenders alike
  - Monitor remediation efforts
  - Rapid tool development cycle to support new deployments

---

### 2015 Toolset

<table>
<thead>
<tr>
<th>Initial Compromise</th>
<th>Maintain Presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>COZYCAR SWIFTKICK / MINIDIONIS</td>
<td>SEADADDY SAYWHAT QUEENPIECE HAMMERTOSS Powershell</td>
</tr>
</tbody>
</table>
Generic Spearphishing

- 2014 – early 2015 Campaign used generic lures / decoys
  - “You’ve got a fax”
  - “Office Monkeys”
- Lure site very relevant
  - Compromised legitimate / prominent sites to deliver “fax”
    - International issues and diplomacy sites
    - European stock exchange
    - US state and local government
    - Prominent US university
- July’2015 campaign showed much more-targeted / topical lures...some generic
APT29’s HAMMERTOSS – Advanced persistent threat

- Backdoor detected in early 2015
- Designed to make it difficult for security professionals to detect and characterize the extent of APT29’s activity.
- Multiple layers of obfuscation
- Mimicking the behavior of legitimate users:
  - Usage of commonly visited websites: Twitter, GitHub, and cloud storage services
FireEye Threat Intelligence Sources

<table>
<thead>
<tr>
<th>Collected</th>
<th>Generation Methods</th>
<th>400,000 unique daily malware samples</th>
<th>Detects</th>
<th>Context Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Malware Collection</td>
<td>10,000 malicious identifiers detected daily</td>
<td>• Botnets, Commodity malware, C2 callbacks</td>
<td>Malware family name, Risk score</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Curated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Team of security experts put intelligence into context</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Focused Rule Sets &amp; IOCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Detection Hunt team monitors for current threats and generate rule packs &amp; IOCs to assist with detection</td>
</tr>
</tbody>
</table>
Using Cyber Threat Intelligence to Enhance Security

- What is Intelligence?
- Why is Cyber Threat Intelligence important?
- Leveraging Cyber Threat Intelligence
  - Enhance security technologies
  - Streamline processes
  - Improve security programs
- iSIGHT Offerings
- Case study
- Questions
WHAT IS INTELLIGENCE?
Cyber Threat Intelligence - Definition

- Intelligence is information that has been collected, processed and disseminated with the purpose of:
  - Reducing the degree of uncertainty about an adversary, potential adversary, situation or threat, which may be experienced by decision makers.
  - So they can make informed, reasoned, and timely decisions.
Cyber Threat Intelligence - Definition

Not to be confused with:

“Information is unprocessed data of every description that may be used in the production of intelligence. It is normally collected by individual sensors, systems or capabilities.”
The Intelligence Cycle – Simple Version

- Direction
- Collection
- Dissemination
- Processing
The Full Intelligence Cycle

- **Requestor/User**
  - Intelligence Requirements (Standing and Priority)

- **Direction**
  - Collection Plan
  - Requests for Information
  - Tasks
  - Task Collection

- **Collection**
  - Information & Intelligence
  - (Time) Critical Intelligence

- **Processing**

- **Dissemination**
FireEye iSIGHT
200+ intelligence Professionals, 29 Languages, 18 Countries

Global Insights

✓ ADVERSARY FOCUSED
✓ GLOBAL COLLECTION
✓ CONTEXTUAL
✓ MULTIPLE DELIVERABLES
✓ PARTNERSHIP
✓ ACTIONABLE

Global Reach
Cyber Threat Intelligence Production
Formal Process Yields Rich, Contextual Threat Intelligence

Direction and Collection
Intelligence Requirements requested from Client
Intelligence Requirements created based on Clients, Sectors and Adversaries
Requirements prioritized by analysts, matched to current holdings then passed to global research teams
Collection planning and tasking of global research teams

Feedback & Clarification

Analysis
Requirements collected by global research teams and returned to Fusion Centre
Processing and exploitation to standardize multiple information sources ready for analysis
Analysis of information and production of reporting for clients

Dissemination
Fully fused, corroborated, cross-referenced and edited multi-source Intelligence reporting disseminated to clients
Client feedback, refinement of Intelligence product
Cyber Threat Intelligence Process

Collection - Global Intelligence Gathering

Collection systems and research team create raw observables...

Common Data Model (ensures consistency)

Processing and Analysis

Campaigns
Actors
Linked Observables
Attack Methods

Deliverable Formats
- HTML or plain-text via email
- Portal access with advanced search capability
- XML delivery
- Indicator CSVs linked to intelligence context
- API access
- Partner Integrations

Content Management System
Coordination, deduplication, topic selection, production, storage and retention of sources

Utilized to create tagged, categorized “wires” or research elements...

Which flow to analytical tools to enrich, prioritize, rate and synthesize our knowledge into...

Finished intelligence which is produced and delivered in many formats to the customer.
WHY IS CYBER THREAT INTELLIGENCE IMPORTANT?
Cyber Threat Joins the Risk List

Key Risks

- Political
  - Supply Chain
  - Regulatory
- Reputation
  - Market
  - Credit
- Environmental
  - Financial
  - Ethics
- Cyber
  - Natural Disasters
  - State Conflicts
How Can Cyber Threat Intelligence Help?

1. Be Proactive
2. Shrink the Problem
3. Improve Prioritization
4. Enhance Executive Communications
5. Connect Security With Business

Actionable Intelligence is:
• Accurate
• Aligned with your intelligence requirements
• Integrated
• Predictive
• Relevant
• Tailored
• Timely

Rick Holland
Blog: Actionable Intelligence, Meet Terry Tate, Office Linebacker
Published: 11 February 2014
LEVERAGING CYBER THREAT INTELLIGENCE
Leveraging CTI to “Shrink the Problem”

Impact of *Context Rich* Cyber Threat Intelligence
 Benefit to Multiple Intelligence Consumers

Strategic

CISO & Executive

Threat Intelligence Team

Operational

Security Operations Center (SOC)

Incident Response Team

Tactical

Network Operations

Systems/Endpoint Operations
Actionable Threat Intelligence

ACROSS THE INFRASTRUCTURE

ThreatScape® API

**ACTIVITY**

- SIEM/Log Management
  - Event Prioritization

- Threat Intelligence Platform (TIP)
  - Threat Data, Indicator Aggregation, Common Platform

- Endpoint Protection
  - Protection for Enterprise Endpoints

- Network Protection
  - Visibility and Protection Across Enterprise Networks

- IR/Forensics Investigations
  - Hunt for Issues, Remediate & Attribute

- Analytics/GRC
  - Analyze Incidents (Who, Why) Patch Management

**VALUE**

- Shrink The Problem
- Manage All Threat Data and Sources in a Single Interface
- Stop Attacks at the Point of Entry
- Alert and Block Threats, Detect Attacks in Progress
- Improve Decisions Who/Why Attack Brief Executives
- Improve Decisions Prioritize Most Critical Patches

Copyright © 2015, FireEye, Inc. All rights reserved. CONFIDENTIAL
Intelligence-Led Security – From the Outside In

**Attack Surface**
- Credit Card Data
- Documents
- Intellectual Property
- PII
- User Logins
- Operational Control
- System Availability

**Attack Methodology**
- A/V
- Access Logs
- IDS
- IPS
- SEIM
- DLP
- Insider Threat

**Threat Sources**
- Intrusion Teams
- Cyber Espionage
- Cyber Crime
- Organized Crime
- Hacktivism
- Activist Groups
- Insiders
- Enterprise IT
- Phishers
- DDoS
- Mobile Computing
- Bot Herders
- Black Hats
- Industrial control sys

**Indicators**
- Tor
- Comms
- Malware
- Botnet
- C2
- Exfil
- Drop
- Exploit

**Indicators, Tags, Actors**
- Anonymity
- Scaling
- Watering Hole
- Direct Intrusion
- Exfiltration
- Social Engineering
Cyber Threat Intelligence

Indicators/IOCs
- Malicious Files (hashes/signatures)
- Bad Domain
- Bad IP Address
- Phishing Lures
- Registry Settings

Context
- Motivation/Intent
  - Cyber Crime (Money)
  - Espionage (Information)
  - Hacktivism (Influence)
  - Destruction (Kinetic Impact)

- Actors
- Attribution
- Targets
- Campaigns
- TTPs, Methods/Playbooks

Motivation/Intent

Copyright © 2015, FireEye, Inc. All rights reserved. CONFIDENTIAL
Last month we:
- Reviewed 1,452,134 log entries
- Detected 423,132 viruses
- Blocked 2,028,43 connections
- Closed 3,095 incident tickets

Last month we detected and blocked two cybercrime attacks linked to a criminal organization in Eastern Europe that has been targeting POS systems at mid-sized retailers. Our actions:
- Prevented the theft of 10 million customer credit card numbers
- Avoided $78 million in lost revenue and the costs that would have been incurred for notifying customers of the data breach, cleaning up infected systems, and paying regulatory fines and legal fees.
Aims of Cyber Threat Intelligence

- Enable proactive, risk-based resource allocation
- Shrink the problem
- Improve prioritization
- Enhance executive communications
- Connect security with business
CASE STUDIES
Cyber Threat Intelligence in Action

- Sample Sandworm open source reports 13 – 16 October 2014.
Cyber Threat Intelligence in Action

**Timeline**

**2009**
- Genesis of SandWorm Team dates to as early as 2009

**Late 2013 and throughout 2014**
- Monitoring of SandWorm Team
- Traced to 2009
- Increased activity throughout 2014

**May 2014**
- GlobeSec attendees targeted

**June 2014**
- Western European government agency
- Polish energy firm targeted (CVE-2013-3906)
- BlackEnergy variant w/Base64-encoded reference to French telecomm firm

**September 2014**
- Zero-day artifacts captured (CVE-2014-4114)
- Spear-phishing email/exploit targeting Ukrainian government
- Coinciding with NATO summit on Ukraine in Wales
- At least one US org fell victim (think tank/academia)

**September 3, 2014**
- ISIGHT Partners labs discovers zero-day vulnerability
- Immediately notified targeted parties and clients across government and private sector domains

**September 5, 2014**
- Began working with Microsoft
- Provided technical analysis of vulnerability and malware used in exploit
- Coordinated tracking of campaign
  - Monitoring for broader targeting and victimization
  - Monitoring for broader use of zero-day exploit in the wild

**Purposefully timed disclosure to coincide w/ MSFT patch release**
- Minimizes potential for copy-cat exploit creation
- Limits exposure to a broad reaching, severe vulnerability
Cyber Threat Intelligence in Action

- **18 Nov 15**, Sandworm Team tied to broader operation targeting ICS Networks using BlackEnergy
- **25 Nov 15**, US academic research and development community targeted with repurposed Sandworm Team exploit
- **30 Mar 15**, Changes to BlackEnergy demonstrate EU focus
- **12 Jun 15**, BlackEnergy 3 malware used by Sandworm Team is capable of leveraging RPC over SMB for both local and remote connections.
- **30 Dec 15**, Cyber Espionage activity in Ukraine resembles sandworm team and nation-wide power outages in Ukraine caused by cyber attacks.
- **24 Jan 16**, Spear phishing targeting Ukrainian energy sector distributed GCat Malware; May indicate sandworm team operators are shifting tools
- **29 Feb 16 and 17 Apr 16**, Sandworm Team campaign leveraged searchable sensitive documents to target Ukrainian media, Boryspil Airport prior to destructive attacks
Questions

iSIGHT Partners
The Cyber Threat Intelligence Experts
Please take a copy

Available to download at: http://info.isightpartners.com/definitive-guide