Discover Smarter Intelligence
AGENDA

Prepare for Cyber Attacks with the Right Intelligence – Greg Day, VP&CTO EMEA

Threat Intelligence – How we do it – Jen Weedon, Threat Intel Manager

Seamlessly Integrating Actionable Intelligence – Josh Goldfarb, CTO Americas

How Actionable Intelligence can Drive Smarter Decisions – Jens Monrad, Systems Engineer
Learn how organisations can prepare for cyber attacks with the right intelligence

Greg Day, CTO EMEA
FireEye Adaptive Defense

INTELLIGENCE
- DISCOVERED 16 OF THE LAST 22 ZERO-DAYS
- "FRONT LINE" INTEL FROM INCIDENT RESPONSE
- MILLIONS OF NETWORK & ENDPOINT SENSORS
- HUNDREDS OF INTEL AND MALWARE EXPERTS
- HUNDREDS OF THREAT ACTOR PROFILES

TECHNOLOGY
- IDENTIFIES KNOWN, UNKNOWN, AND NON MALWARE BASED THREATS
- INTEGRATED TO PROTECT ACROSS ALL MAJOR ATTACK VECTORS
- PATENTED VIRTUAL MACHINE TECHNOLOGY

EXPERTISE
- "GO-TO" RESPONDERS FOR SECURITY INCIDENTS
- HUNDREDS OF CONSULTANTS AND ANALYSTS
- UNMATCHED EXPERIENCE WITH ADVANCED ATTACKERS
What’s your most scarce Cyber Security resource?
M-Trends 2015

How Compromises Are Being Detected

31% victims discovered the breach internally

69% victims notified by an external entity

Time from Earliest Evidence of Compromise to Discovery of Compromise

205 median number of days that threat groups were present on a victim's network before detection

24 days less than 2013

Longest Presence: 2,982 days
The Numbers Game – IDG & FireEye report

- 37% of organisations have over 10,000+ security events per month.
- 64% of the alerts were redundant.
- Over 40% of companies manually review each alert.
- 52% of alerts being false positives.

2020 = 5-10x IP addresses
Bland intelligence or Contextual & Rich

“The four most common types of data offered in commercial threat intelligence include hashes, IP addresses, domain names and URLs. The reason these data types are most common is because of easy standardization and the ability to collect them at scale”

IDC Predictions 2015: Accelerating Innovation — and Growth — on the 3rd Platform

“Threat intelligence data services provide a better understanding of the active tools, targets, and campaigns of IT and communication system attackers and are a key component in predicting the probability of specific attacks.

IDC predicts that, by 2017, 55% of enterprises will receive tailored threat intelligence information”
Ave. 74% attacks are custom designed & unique
(% of number instances of each attack per company by month first seen)

Ave. 99,000 unique samples per month
# Leaning Forward With Intelligence

**What is it?** - “Threat Intelligence”

You need to think more critically…

<table>
<thead>
<tr>
<th>TACTICAL INTELLIGENCE</th>
<th>CONTEXTUAL INTELLIGENCE</th>
<th>STRATEGIC INTELLIGENCE</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Tactical Icon" /></td>
<td><img src="image2.png" alt="Contextual Icon" /></td>
<td><img src="image3.png" alt="Strategic Icon" /></td>
</tr>
</tbody>
</table>

**Tactical intelligence** is automatically generated from local deployments. When a system analyzes a suspicious file and discovers a new malware variant, for instance, it can generate and quickly distribute a new indicator of compromise (IOC) to inoculate the entire enterprise.

**Adaptive architectures** also incorporate contextual intelligence from research labs and incident responders for a broader view of attack trends and detailed profiles of attackers and their methods.

**Strategic intelligence**—typically from threat bulletins, industry briefings, and the like—give security leaders information for longer-term planning, management, and budgeting.
Threat Intelligence – How We Do It

Jen Weedon, Manager, Global Threat Intelligence and Strategy
WHAT IS THREAT INTELLIGENCE?

- “Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject’s response to that menace or hazard.”

  - Gartner Research
FIREEYE INTELLIGENCE TEAM

About Us
Threat Intelligence Mission

- Track, research, and analyze cyber threats
- Centralize and disseminate our data and findings
- Equip customers with a decision-making edge at the tactical, operational, and strategic levels
- Help position the use of threat intelligence in our products and in our corporate strategy
3 Pillars of Good Threat Intelligence

People

Data

Technology
FireEye and Mandiant Sources

Mandiant Investigations
- **450+** Clients
- **24** of the Fortune 100
- **74** of the Fortune 500
- **7 of 10** Largest Defense Contractors
- **30+** Industries

FireEye Customers in 2-Way Mode
- 3,000+ customers across more than 60 countries, including over 130 of the Fortune 600

External Relationships
- Malware Feeds
- Open Source Research
OUR PROCESS

1. Identify objectives
   - Collect required data
     - IR sources
     - Sensors in the field

2. Consumption of data sources into analytics database

3. Model infrastructure and tools
   - Track targeting preferences and types of asset targets
   - Anticipate target trends and emerging threats

4. Intelligence delivered as either machine-consumed intelligence or strategic level reports
OUR ANALYSIS

MODEL THE INFRASTRUCTURE AND TOOLS

TRACK TARGETING PREFERENCES AND TYPES OF ASSET TARGETS

ANTICIPATE TARGET TRENDS AND EMERGING THREATS

SPONSOR ATTRIBUTION
Attrition of Threat Groups

- Understand who the adversaries are, categorize what they are after and the risks the pose.
- Many threat actors share the same set of tasks, tools and methodologies and coordinate on targets.
- Attribution is still possible based on analytical experience, proprietary tools and forensic evidence left behind.
- Evidence must show beyond a reasonable doubt that intrusion events are related.
INTELLIGENCE IN ACTION: APT30

APT30 AND THE MECHANICS OF A LONG-RUNNING CYBER ESPIONAGE OPERATION

How a Cyber Threat Group Exploited Governments and Commercial Entities across Southeast Asia and India for over a Decade
Considerations

- Data / visibility is key
- No one knows it all, or even close
- Your system must be resilient to analyst turnover, so your data and findings must be self explanatory
- Your system needs to record the logic that justified a decision and needs to be able to reverse that decision
- Different data and different threats require different approaches and technology
Seamlessly Integrating Actionable Intelligence

Josh Goldfarb, CTO Americas
Agenda

- Collect
- Vet
- Retain
- Leverage
Collect

- Choose wisely
- Consider risks to mitigate
- Cover different perspectives
- Quality over quantity
Vet

- Context
- Source
- Reliability
- Noise
Retain

- Use once vs. Re-use
- Granularity of retention important
- Metrics on indicators and families of indicators
- Metrics on sources
- Metrics on impact
- ROI
Leverage

- Integrate seamlessly into workflow
- Hard to do means won’t do
- Automation
- What goes in must come out
- All about the workflow
Questions?
UNDERSTAND HOW ACTIONABLE INTEL CAN DRIVE SMARTER DECISION MAKING

Jens Monrad, Systems Engineer
## FireEye Threat Intelligence Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Dynamic Threat Intelligence (DTI)</th>
<th>Advanced Threat Intelligence (ATI)</th>
<th>Advanced Threat Intelligence Plus (ATI+)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Intel Updates for FireEye Platforms</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>One- and Two-Way Threat Intelligence Sharing</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Community-Based Intel Sharing</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Attribution of Alerts to Known Threat Actors</td>
<td>●*</td>
<td>●*</td>
<td>●*</td>
</tr>
<tr>
<td>Description of Malware Family</td>
<td>●*</td>
<td>●*</td>
<td>●*</td>
</tr>
<tr>
<td>Vulnerability and Kill Chain Analysis</td>
<td>●*</td>
<td>●*</td>
<td>●*</td>
</tr>
<tr>
<td>Continuous Monitoring by FireEye Analysts</td>
<td></td>
<td>●*</td>
<td>●*</td>
</tr>
<tr>
<td>Detection Efficacy Monitoring</td>
<td></td>
<td>●*</td>
<td>●*</td>
</tr>
<tr>
<td>Detailed Information on Malware Families</td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Enriched Community Intel Sharing</td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Threat Actor Profiles</td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>In-Depth Analysis and Reports on Attacker Trends</td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>On-Demand Analysis of IPs and Domains</td>
<td></td>
<td>●</td>
<td>●</td>
</tr>
</tbody>
</table>

* is only available in Two-Way Threat Intelligence Sharing mode.
# Advanced Threat Intelligence

## Event Summary

**Name:** Infostealer.DTI.POSMalware  
**MD5 SUM/URL:** cee0296e2d77ec3bb112e270fc260f274  
**Threat Level:** High  
**Attribution:** Infostealer.DTI

**Mitigation:** Data not available

## Indicator of Compromise

**Command Executed:**
- `cmd /c net start POSWDS`  
- `%SystemRoot%\system32\cmd.exe /c net use S: \10.116.240.31\c$\WINDOWS\twain_32 /user:ttcopsdl3scpt\Best1_user BackupUser$`  
- `%SystemRoot%\system32\cmd.exe /c move %SystemRoot%\system32\winxml.dll S:\Server PC_15_1_15.txt`  
- `%SystemRoot%\system32\cmd.exe /c net use /del`  
- `C:\exec\{MALWARE}.exe (cee0296e2d77ec3bb112e270fc260f274)`

**Dropped Files:**

## Software Mitigation

**Data not available**

## Threat Lifecycle

**Installations:**
- Process starting system services  
- Process create network share  
- Process move system files  
- Process delete network share  

**Delivery:**
- Email Attachment

## Malware Exploit Details

**Data not available**
ATI+ - leaning forward with intelligence
Risk Snapshots: Mobile Devices and Targeted Threats

Introduction Employees often use personal devices for work-related issues, a common practice referred to as Bring Your Own Device (BYOD). The use of personal devices — such as smartphones, tablets...

Risk And Targeting Profile

Suspected Russian Cyber Criminals Use Click-Fraud to Propagate Pro-Russia Media

Summary On April 23, 2015, Trend Micro's SpiderLabs released a blog describing suspected Russian...

Risk And Targeting Profile

Ticket Please: Multiple Threat Actors Leverage Kasbar

Cyber Threats to the Nordic Region

We have observed APT18 conduct network intrusions against a wide variety of targets, including the defense industrial base, health care, computer software, non-governmental organizations, and financial services. APT18 actors have also targeted electronic organizations specializing in law enforcement-related surveillance technologies, probably to collect sensitive information accelerating Chinese capabilities. These technologies can enhance intelligence, surveillance, and reconnaissance platforms as well, which we have seen APT18 target. Many APT18 spear-phishing messages are crafted to appear sympathetic to attacked individuals or departments within the victim’s own company, it may claim to contain or point to a software update. APT18 threat actors have also sent malicious links to potential victims via chat or instant messaging. APT18 uses a variety of backdoors, including publicly available tools and custom backdoors. FireEye Labs has identified a small number of cases where APT18 actors signed malicious code using a valid code-signing certificate stolen from a US-based company.

APT18 Tactics, Techniques, and Procedures (TTPs)

The following sections describe APT18 tactics, techniques and procedures, and are organized according to the stages of Mandiant’s Chinese APT Attack Lifecycle model. These descriptions are based on Mandiant’s own observations and research; the amount of available data may vary based on our visibility into a particular threat group. Where no specific information is provided, either the group’s behavior is not distinctive (i.e., it corresponds to the Chinese APT Attack Lifecycle) or only limited information is known at this time.

Initial Compromise

Methods are consistent with the standard APT attack lifecycle. Like most APT groups, APT18 typically uses spear-phishing messages with malicious attachments or links to malicious files or web sites. Many APT18 spear-phishing messages are crafted to appear sympathetic to attacked individuals or departments within the victim’s own company, it may claim to contain or point to a software update. APT18 threat actors have also been known to send malicious links to potential victims via chat or instant messaging. Finally, they may attempt to identify vulnerable web servers within a target network’s demilitarized zone (DMZ) and exploit vulnerabilities to gain access to the network.

For examples of APT18 spear-phishing, see “Multiple Organizations Phished for Credentials by APT18 Actors,” or “APT18 Spear Phishing Campaign Entices Users to Download and Install an Alleged Software Update.”

Establish Foothold

APT18 threat actors use a variety of backdoors, including publicly available tools such as GHOST RAT and PHOENIX (IV), custom backdoors that are also used by other APT groups (such as HUSKYSNAP), and custom backdoors that do not, have only been obtained in use by APT18 (to include MUSK), Mandiant has identified a small number of cases where APT18 actors signed malicious code using a valid code-signing certificate stolen from a US-based company. However, code signing appears to be an exception with this actor.

Escalate Privileges

Methods are consistent with the standard Chinese APT attack lifecycle. APT18 actors may use modified versions of publicly available tools such as pwdump and the pass-the-hash tool. 
Managing Intel in FIC

- Built-in indicator extraction
- Versioning of intelligence documents
- Seamless sharing with internal or external constituents
- API access in Q3 2015
- Free!
  - Customers get enrichment; anyone can manage/share
- Contact your account executive today to try it
## FIREEYE THREAT INTELLIGENCE FEATURES

<table>
<thead>
<tr>
<th></th>
<th>TWO WAY</th>
<th>ONE WAY</th>
<th>OFFLINE PORTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTI</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>ATI</td>
<td>✔️</td>
<td></td>
<td>✔️</td>
</tr>
<tr>
<td>ATI+</td>
<td>✔️</td>
<td>✔️</td>
<td>✔️</td>
</tr>
</tbody>
</table>
Industry’s best threat intelligence, applied to event data

- 3M+ indicators
- 900+ proprietary rules
- Tight integration with FireEye Intelligence Center for context
- Analytics provides heuristic detection
- Integrates with other FireEye products

Hosted Solution

- One price for infrastructure, management, software license
- Scalable event consumption
- Minimal onsite configuration

Fast response

- Sub-second search across billions of events
- Pivoting and grouping to facilitate hunting
- Integrated case management
FIREEYE AS A SERVICE

MVX EVERYWHERE

ENDPOINT SECURITY REIMAGINED

CONNECTING THE DOTS

GLOBAL THREATSCAPE VIEW

OPERATING SYSTEMS

SECURITY

ULTRAVISOR

EXPLOIT AND MALWARE DETECTION

FORENSICS AND VALIDATION

WHITE-LISTING AND BLACK-LISTING

INVESTIGATION MANAGEMENT PLATFORM

ANSWERS, NOT ALERTS

INTELLIGENCE

Copyright © 2015, FireEye, Inc. All rights reserved.
Questions?