2016 THREAT ENVIRONMENT

UNRESTRAINED ADVERSARIES POINT WAY TO MORE DIVERSE THREAT LANDSCAPE

MARCH 23, 2016

Presented by Christopher Porter, Senior Threat Intelligence Analyst, to the Information Security and Privacy Advisory Board

FireEye®
SECURITY REIMAGINED

Key Findings

- The lack of effective cyber deterrence has emboldened Advanced Persistent Threat (APT) groups.
- Sophisticated groups do not rely on zero days—they can turn the operating system against itself.
- Commoditization of cybercrime has spread APT-like threats worldwide.
- Threat groups are figuring out the formula for causing critical infrastructure outages.
- Threat to mobile likely to rise precipitously following FBI case against Apple.
- Intelligence sharing—information in context—is necessary to improve protection against cyber threats.

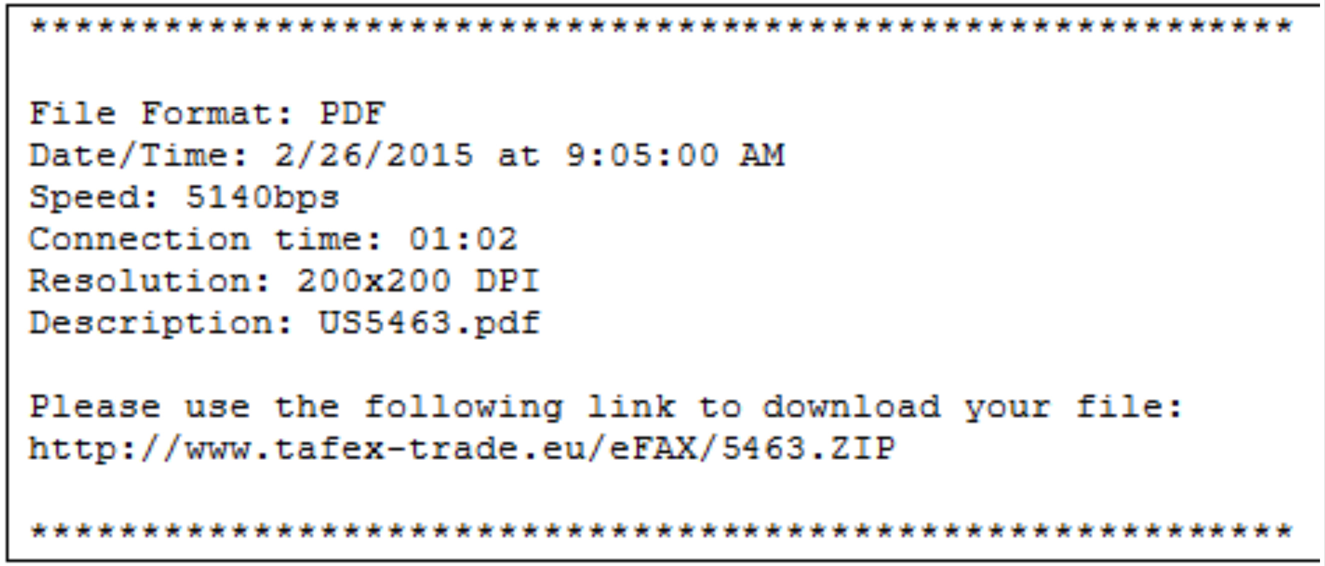
Game Theory for State-Sponsors of Cyber Attacks Now Favors Offense Rather Than Restraint

- Over the past year, public discussion of cyber attacks has turned to how major destructive attacks have gone unpunished and the difficulties of confident attribution.

- State sponsors of hacking worldwide probably now assess that they can conduct even destructive operations without provoking physical or significant economic responses from their targets.

- **APTs are continuing their operations even after detection and attribution.**

Dangerous Theory in Practice: APT29

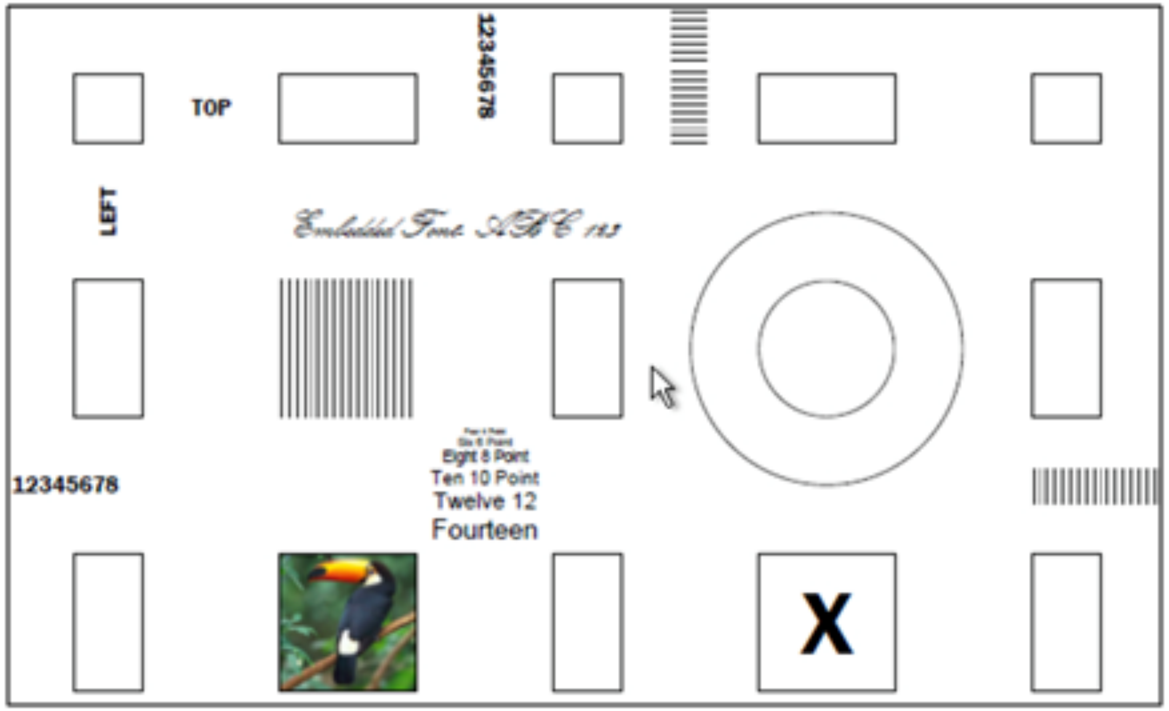


```
*****************************************************************

File Format: PDF
Date/Time: 2/26/2015 at 9:05:00 AM
Speed: 5140bps
Connection time: 01:02
Resolution: 200x200 DPI
Description: US5463.pdf

Please use the following link to download your file:
http://www.tafex-trade.eu/eFAX/5463.ZIP

*****************************************************************
```



- Cybercrime-style phishing emails
- Western national governments and foreign policy entities, media organizations, defense and government contractors, and higher education institutions.
- Targeting geopolitical information related to Ukraine conflict
- Operations and development occur in Moscow time

Dangerous Theory in Practice: APT29, continued

- Email links to legitimate, compromised websites
- Real voicemails used as lures
- Escalates privileges using built-in and publicly available Windows administration tools **without writing to disk.**
- Malicious commands run as scheduled tasks.
- **Threats like APT29 must be actively hunted for to discover them; passive, network-edge detection will not work.**

Dangerous Theory in Practice: APT29, continued

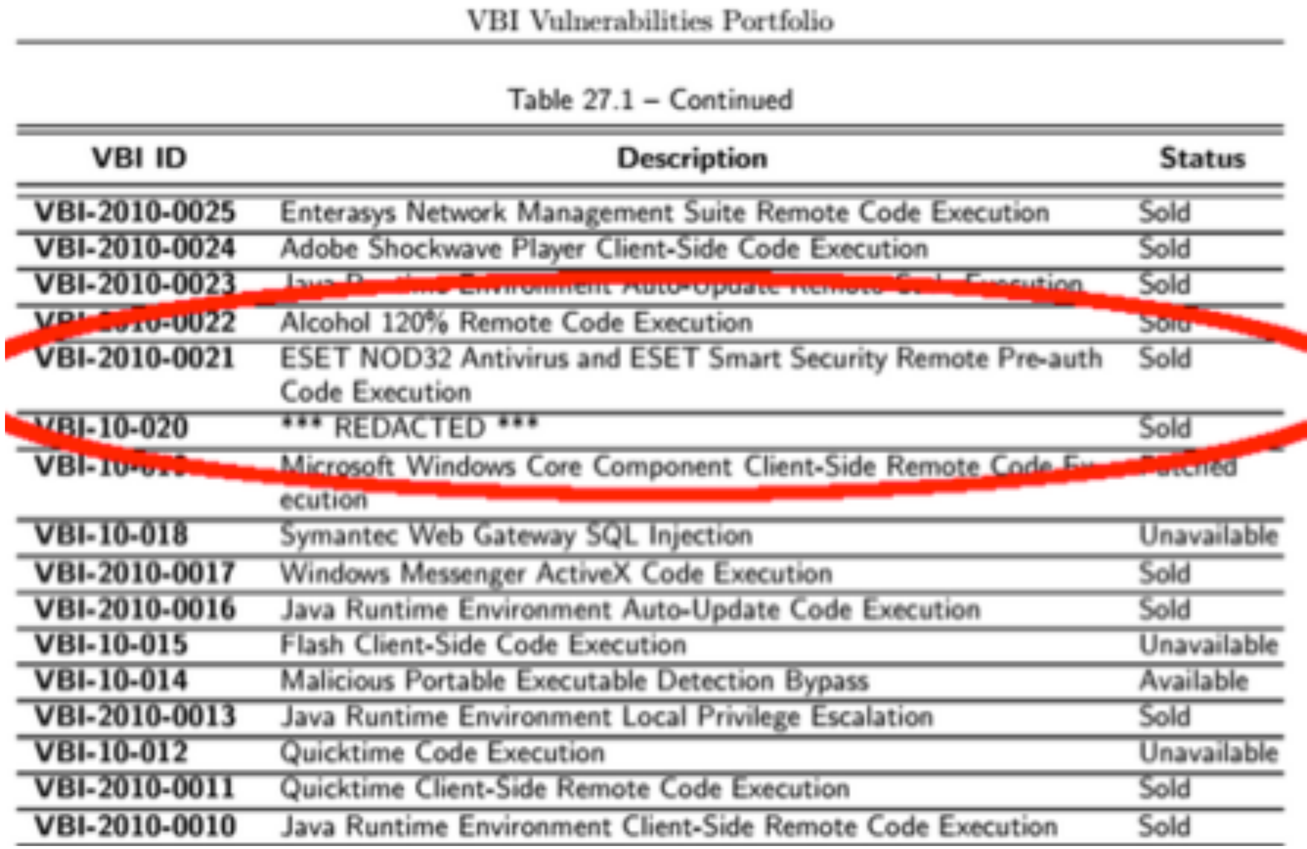
- APT29 operators operated with a full understanding that investigations were underway and defenders were watching.
- Repeated exposure and indicator sharing did not even slow them down.
- APT29 learned of an upcoming remediation event and obtained fresh password dumps in order to acquire the latest passwords.
- **Lesson learned: importance of out-of-band emergency security line.**

The Digital Underworld is Flat: Cybercrime Market Matures

- Offensive tool vendors—“legitimate” and underground—give even small nations and criminal groups the purchasing power to keep up a steady supply of zero days.

- Hackers can threaten anyone from anywhere…(driving prices down and threats up)

- ...but geography still matters. Cybercriminals in Latin America, Middle East, and Eastern Europe often operate with impunity in the absense of laws and enforcement capability.



VBI Vulnerabilities Portfolio

Table 27.1 – Continued

VBI ID	Description	Status
VBI-2010-0025	Enterasys Network Management Suite Remote Code Execution	Sold
VBI-2010-0024	Adobe Shockwave Player Client-Side Code Execution	Sold
VBI-2010-0023	Java Runtime Environment Auto-Update Remote Code Execution	Sold
VBI-2010-0022	Alcohol 120% Remote Code Execution	Sold
VBI-2010-0021	ESET NOD32 Antivirus and ESET Smart Security Remote Pre-auth Code Execution	Sold
VBI-10-020	*** REDACTED ***	Sold
VBI-10-019	Microsoft Windows Core Component Client-Side Remote Code Execution	Patched
VBI-10-018	Symantec Web Gateway SQL Injection	Unavailable
VBI-2010-0017	Windows Messenger ActiveX Code Execution	Sold
VBI-2010-0016	Java Runtime Environment Auto-Update Code Execution	Sold
VBI-10-015	Flash Client-Side Code Execution	Unavailable
VBI-10-014	Malicious Portable Executable Detection Bypass	Available
VBI-2010-0013	Java Runtime Environment Local Privilege Escalation	Sold
VBI-10-012	Quicktime Code Execution	Unavailable
VBI-2010-0011	Quicktime Client-Side Remote Code Execution	Sold
VBI-2010-0010	Java Runtime Environment Client-Side Remote Code Execution	Sold

“But Cybercriminals Are Not APTs: What’s the Worst That Could Happen?”

- **False Flag Attacks -** Criminal groups have APT-like capabilities and go after similar targets. Both know that defenders will have a hard time telling them apart. *Large-scale cybercrime must be reduced to even begin addressing APT incentives.*

- **Targeting the Executive –** Attacking leadership at home or on mobile devices as an entry vector to organization or for digital blackmail. *Cyber is often tactically “symmetric” even when it is strategically asymmetric.*

- **Consequences Spiral –** Ransomware designed for profit disables far more than threat actors intend (or not), resulting in loss of physical infrastructure operation or life. *Operational savvy, not cyber skill, is “limiting reagent” for ICS attacks. These incidents enable criminals and APTs alike to learn what works.*

Precedents Being Set are Worsening Threats to Mobile

- FireEye tracks 15 different Chinese APTs that conduct computer network operations against telecommunications companies worldwide.
- Two Chinese APTs, APT1 and APT5, have targeted mobile operators' intellectual property, including code.
- Several Russian groups already exploit jailbroken iOS.
- Celebrity photo-scandal actors relied on "law enforcement-only" tool and brute force password-guessing.
- China as of 1 January requires companies operating there to provide technical assistance "to avert and investigate terrorist activities."
- FireEye tracks 9 Chinese APTs that target NGOs, ethnic and religious minorities, and related news outlets that would probably fall under this law.

Intelligence Sharing—Not Information Sharing—Key to Improving Public-Private Cyber Defense Partnerships

- APT29 exposed more than a dozen times over 18 months, with no demonstrable effect on their operational tempo.
- Indicators may be necessary, but they are not sufficient.
- Best groups will leave indicators behind to dazzle technology-only solutions and mislead non-expert investigators.
- APTs are also informed when information is broadly shared.
- Indicators combined with context, like plans and intentions or attribution, can help private sector prioritize engagements, identify unique activity, and provide more valuable information back to public sector.

Questions?

- Christopher.Porter@fireeye.com