



State of the Hack

Observations from Mandiant Investigations

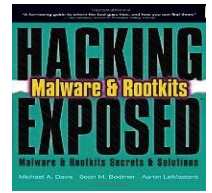
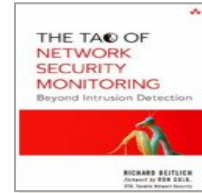
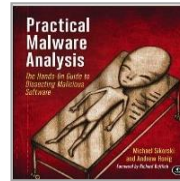
Background

Mandiant

- Based in Washington DC
- Focused on helping organizations recover from security breaches
- Released concrete evidence of hacking by the Chinese PLA
- Significant knowledge of hundreds of threat actors operating across the globe

Charles Carmakal











- Managing Director
- Based in Washington DC
- Over 15 years of experience in incident response and ethical hacking













Agenda

- Who are the threat actors?
- What are the trends?
- How do we combat advanced attacks?
- Q&A

Threat Actor Motivations

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Disruption
Objective	 Access & Propagation	 Economic, Political Advantage	 Financial Gain	 Defamation, Press & Policy	 Escalation, Destruction
Example	Botnets & Spam	Advanced Persistent Threat Groups	Credit Card Theft	Website Defacements	Destroy Infrastructure
Targeted					
Character	Often Automated	Persistent	Frequently Opportunistic	Conspicuous	Conflict Driven

Threat Actor Motivations

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Disruption
Objective	 Access & Propagation	 Economic, Political Advantage	 Financial Gain	 Defamation, Press & Policy	 Escalation, Destruction
Example	Botnets & Spam	Advanced Persistent Threat Groups	Credit Card Theft	Website Defacements	Destroy Infrastructure
Targeted					
Character	Often Automated	Persistent	Frequently Opportunistic	Conspicuous	Conflict Driven

THE WORLD TODAY



May 2014

INDICTMENT OF CHINESE SOLDIERS











US indicts 5 individuals in China's Unit 61398 for cyber-spying on US firms



Chinese Government Motivations

- The intrusions continue...
- Ongoing attacks to give the Chinese government and domestic enterprises an economic, military, or political advantage
- They are known to compromise entities for the following reasons:
 1. Theft of intellectual property
 2. Mergers, acquisitions, and divestments of foreign companies
 3. Modernization of processes and technologies
 4. Political reasons – political activists, spread of democracy, etc.
- They follow their own rules of engagement.

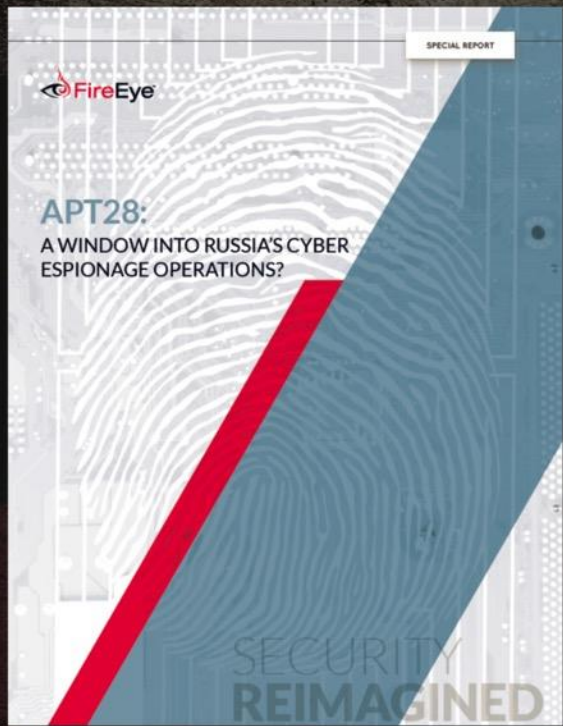
Threat Actor Motivations

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Disruption
Objective	 Access & Propagation	 Economic, Political Advantage	 Financial Gain	 Defamation, Press & Policy	 Escalation, Destruction
Example	Botnets & Spam	Advanced Persistent Threat Groups	Credit Card Theft	Website Defacements	Destroy Infrastructure
Targeted					
Character	Often Automated	Persistent	Frequently Opportunistic	Conspicuous	Conflict Driven

THE WORLD TODAY



RUSSIAN ACTIVITY



● Malware

- Evolves and maintains tools for continued long-term use
- Various data theft techniques

● Targeting

- Georgia and the Caucasus Eastern European governments & militaries
- Security-related organizations

● Russian Attributes

- Russian language indicators
- Malware compile times correspond to work day in Moscow's time zone

POINT OF SALE MALWARE

Ten new POS malware families investigated in 2014

- Backoff POS
- BrutPOS
- Soraya
- Nemanja
- JackPOS
- Decebal
- ChewBacca
- BlackPOS
- Alina
- vSkimmer



FIN4

The screenshot shows a Gmail inbox within an Outlook application window. The interface includes a top navigation bar with 'FILE', 'HOME', 'SEND / RECEIVE', 'FOLDER', and 'VIEW' tabs. Below this is a ribbon with various email actions like 'New Email', 'Reply', 'Forward', and 'Delete'. The left sidebar shows the 'Inbox (315)' and other folders like 'Drafts', 'Sent Mail', and 'Spam'. The main area displays a list of emails with columns for 'From', 'Subject', and 'Time'. The selected email is from 'WinInfo Daily UPDATE' with the subject 'For Windows 8, a Familiar Launch Story'. The preview pane on the right shows the content of this email, including a photo of Paul Thurrott and social media sharing options.

From	Subject	Time
Serge	RE: Just an update	21:36
Where's Willy?	Notification from Where's Willy? Your \$5 bill has been found: APM11--21 Congratulations Your 2006 Five dollar bill with serial number APM11--21	16:49
Canadian Tire Customer Panel	Share your opinions - Rate a magazine cover Hello Matt We have a fun and interactive survey for you. In it, you will be	15:06
Holly	Costume Follow up Hi Matt... This is Holly touching base.	14:20
WinInfo Daily UPDATE	For Windows 8, a Familiar Launch Story View on Mobile Phone	13:29
eBay Member:	sent a message about Other: http://g.ebaystatic.com/aw/parcelpages/eBay_35433.gt	13:15
YouTube Service	sent you a video: http://v.yimg.com/yimg/email/digest/email_header.png	12:14
Mike Elgan	Mike Elgan Daily for 11/19/2012 Mike Elgan Daily	12:04
Nelly	Personal income tax returns Please find attached a copy	11:17
Where's Willy?	Notification from Where's Willy? Your \$5 bill has been found: A4B99--76 Congratulations Your 2006 Five dollar bill with serial number A4B99--76	10:52

WinInfo Daily | UPDATE
For Windows 8, a Familiar Launch Story
By Paul Thurrott

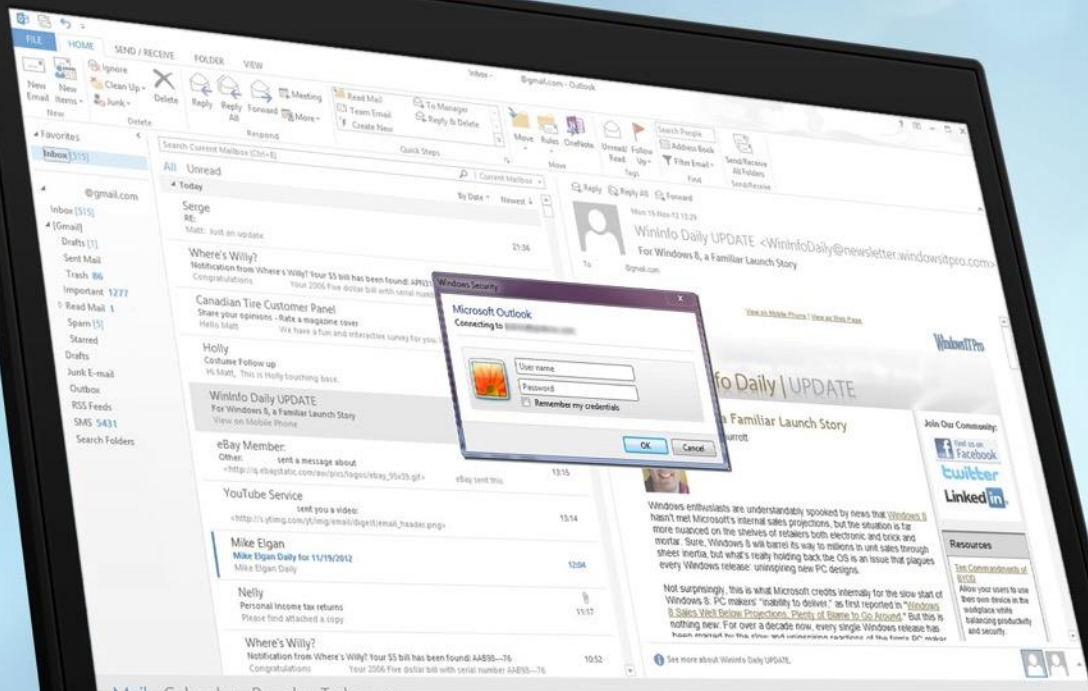
Windows enthusiasts are understandably spooked by news that **Windows 8** hasn't met Microsoft's internal sales projections, but the situation is far more nuanced on the shelves of retailers both electronic and brick and mortar. Sure, Windows 8 will barrel its way to millions in unit sales through sheer inertia, but what's really holding back the OS is an issue that plagues every Windows release: unimproving new PC designs.

Not surprisingly, this is what Microsoft credits internally for the slow start of Windows 8. PC makers' "ability to deliver" as first reported in **"Windows 8 Sales Not Quite Projections, Plenty of Signs to Get Alarmed"**. But this is a sales issue. For over a decade now, every single Windows release has been marred by the other but unmentioned reputation of the former OS' midbar











Join Our Community:
Follow us on Facebook
Follow us on Twitter
Follow us on LinkedIn

Resources
The Commandments of W800
Allow your users to use their own devices in the workplace while balancing productivity and security.

FIN4













Threat Actor Motivations

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Disruption
Objective	 Access & Propagation	 Economic, Political Advantage	 Financial Gain	 Defamation, Press & Policy	 Escalation, Destruction
Example	Botnets & Spam	Advanced Persistent Threat Groups	Credit Card Theft	Website Defacements	Destroy Infrastructure
Targeted					
Character	Often Automated	Persistent	Frequently Opportunistic	Conspicuous	Conflict Driven



SYRIA

Threat Actor Motivations

	Nuisance	Data Theft	Cyber Crime	Hacktivism	Disruption
Objective	 Access & Propagation	 Economic, Political Advantage	 Financial Gain	 Defamation, Press & Policy	 Escalation, Destruction
Example	Botnets & Spam	Advanced Persistent Threat Groups	Credit Card Theft	Website Defacements	Destroy Infrastructure
Targeted					
Character	Often Automated	Persistent	Frequently Opportunistic	Conspicuous	Conflict Driven





조선민주주의



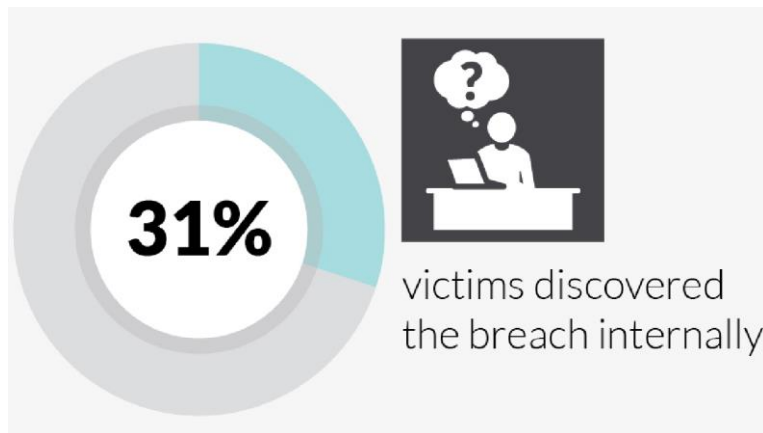
인민공화국만세!

**NORTH
KOREA**

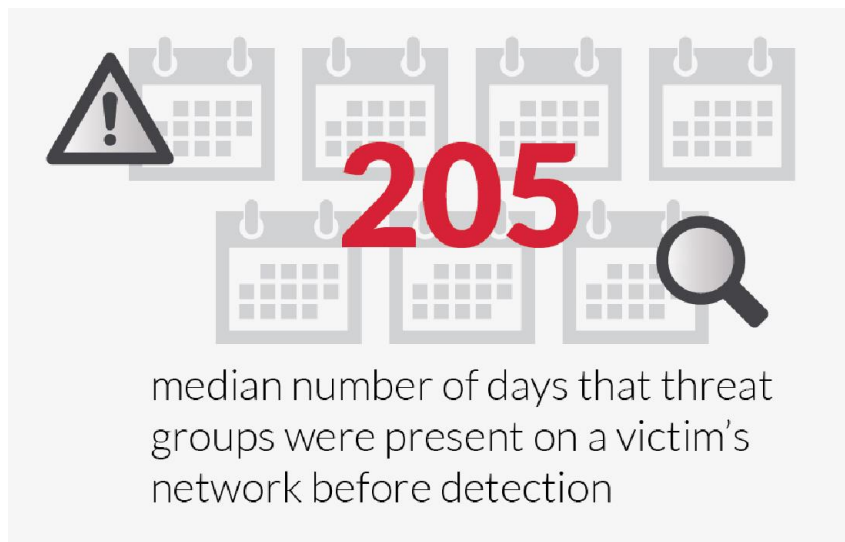
BY THE NUMBERS

The background features a light gray grid pattern that recedes into the distance. A horizontal line is positioned below the title. In the bottom right corner, there is a large, stylized geometric shape composed of a teal triangle and a red triangle.

How Compromises Are Being Detected



Dwell Time



↓ 24 days less than 2013

Longest Presence: 2,982 days

ASSUMPTIONS

- Attacker has domain administrator privileges
- Attacker has hashes or cracked passwords for all domain accounts
- Attacker has additional stolen certificates
- Attacker can freely move
 - VPN to servers
 - VPN to workstations
 - Host to host
- Partner networks may be compromised



APT Phishing



78%

of observed phishing emails were IT or security related, often attempting to impersonate the targeted company's IT department or an anti-virus vendor

72%

of phishing emails were sent on weekdays



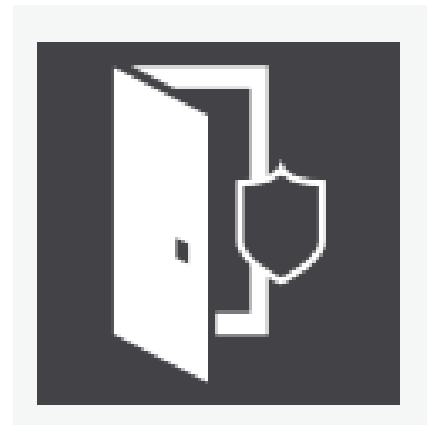
STRUGGLING WITH DISCLOSURE

Trend 1: Struggling with Disclosure

- Mandiant worked with over 30 companies that publicly disclosed a compromise
- Many of them learned about the breach from the media.
- The public is asking more informed questions:
 - Attribution
 - Malware
 - Attacker TTPs
- Public speculation starting to affect investigations

Why the Increase in Notifications?

- Mandiant worked an increased number of cases where protected data was lost
 - Cardholder data, Personally identifiable information (PII), and Protected Health Information (PHI)
 - Contractual and legal obligation to notify
- 69% of victims did not self-detect
 - Increased pressure to notify
- More companies willing to notify
 - Companies feel like it's the right thing to do
 - Being a breach victim is less taboo than in the past



Critical Investigation Questions

- Questions you should have answers to during the investigation
 - How did the attacker gain initial access to the environment?
 - How did the attacker maintain access to the environment?
 - What is the storyline of the attack?
 - What data was stolen from the environment?
 - Have you contained the incident?



The Takeaways

- Breaches are inevitable
 - Have an effective communication strategy available
- Consistent communication is key
 - Based on factual investigative findings
- Public speculation will happen
 - Avoid distracting the investigation



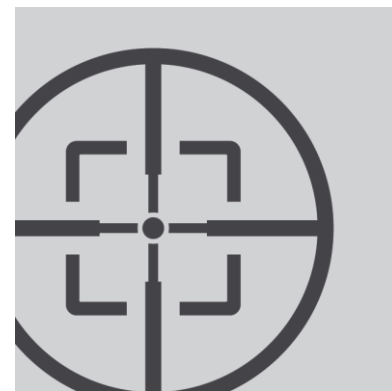
CAUTION
Investigation Hazard

RETAIL IN THE CROSSHAIRS

The background features a light gray grid pattern that recedes into the distance. A horizontal line is positioned below the title. In the bottom right corner, there is a large, stylized geometric shape composed of a red triangle and a teal trapezoid.

Trend 2: Retail in the Crosshairs

- Retailers thrust into the spotlight in 2014
- New groups getting into the game
- Small misconfigurations led to greater compromise



Themes of Financial-Motivated Attackers in 2014

- Citrix servers used as an entry point
 - Valid credentials used to authenticate
 - Misconfigurations / lack of network segmentation allowed greater access
- New tools, tactics, and procedures
 - Highly sophisticated malware
 - Publically available tools
- Increased number of attacks against e-commerce in locations that deployed chip-and-PIN technology
 - Attackers shifting focus to lowest hanging fruit

Initial Access To Environment

- Attacker authenticated to a Citrix server
 - Already had legitimate credentials, no failed logons
- Escaped from “jailed” environment to gain additional control over the system
- Misconfiguration in virtual application server resulted in greater access to environment
 - No segmentation
- Same local administrator password on all systems
 - Allowed attacker privileged access to systems



Data Theft

- Attacker used domain controller as pivot point into retail environment
 - The retail domain had a two-way trust with the corporate domain
 - The store registers ran Microsoft Windows XP
 - The store registers were joined to the retail domain
- Deployed card harvesting malware to registers throughout the environment
- Malware wrote stolen track data to temporary MSSQL database
- Attacker queried database to collect stolen track data
- Transferred files off of network using FTP, Citrix, and web servers



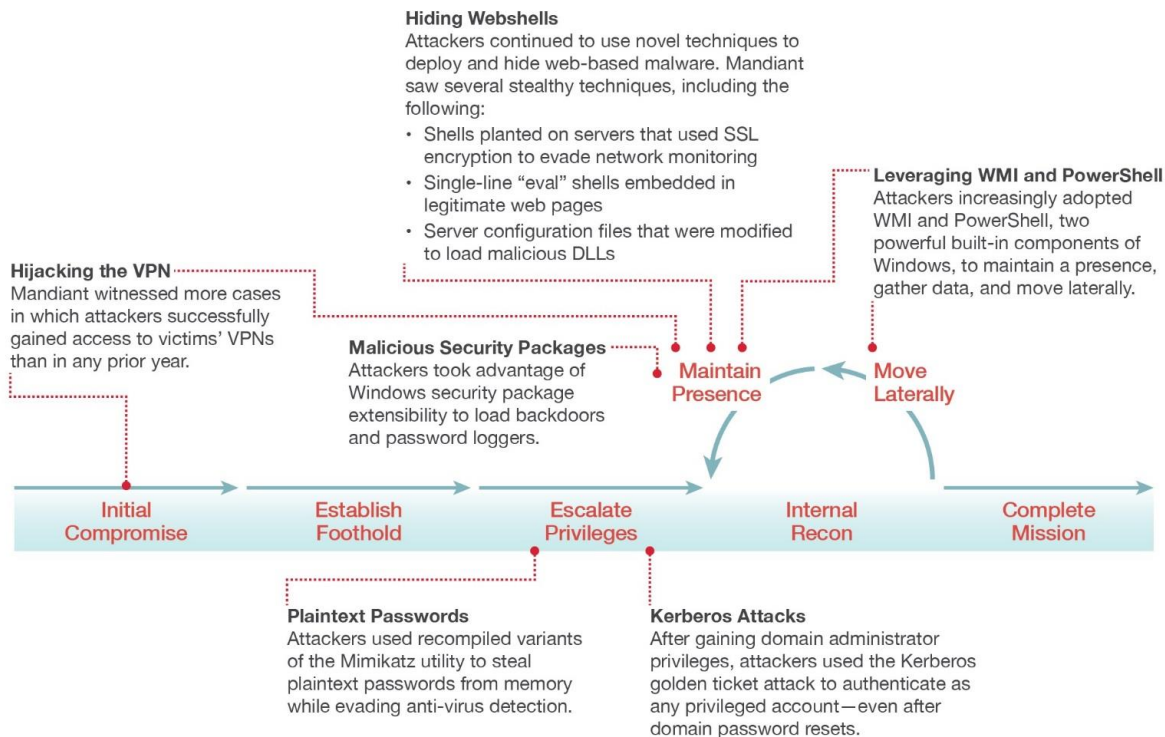
THE EVOLVING ATTACK LIFECYCLE

Trend 3: The Evolving Attack Lifecycle

- Threat actors have used stealthy new tactics to move laterally and maintain persistence in victim environments.



Attack Lifecycle



Hijacking the VPN

- Heartbleed vulnerability
- Single-factor authentication & credential theft
- Bypassing two-factor authentication

```
meterpreter > mimikatz_command -f crypto::exportCertificates CERT_SYSTEM_STORE_CURRENT_USER
Emplacement : 'CERT_SYSTEM_STORE_CURRENT_USER'\My
- developer first
  Container Cl? : c370b0f2969ff11dbc30fef785d9bbdb_abac1a7c-8a16-4f4b-b59d-11a77d0daf3d
  Provider      : Microsoft Enhanced Cryptographic Provider v1.0
  Type          : AT_SIGNATURE
  Exportabilit? : NON
  Taille cl?   : 2048
  Export priv? dans 'CERT_SYSTEM_STORE_CURRENT_USER_My_0_developer first.pfx' : OK
  Export public dans 'CERT_SYSTEM_STORE_CURRENT_USER_My_0_developer first.der' : OK
```

Dumping certificates with Mimikatz (Image Source: www.darkoperator.com)

Password Harvesting

“Victims quickly learned that the path from a few infected systems to complete compromise of an Active Directory domain could be incredibly short.”

- Clear-text passwords in memory
- “Golden Ticket” Kerberos attack
- Malicious security packages



COMBATTING TARGETED ATTACKS

Tactical Steps to Reduce the Risk

Effective Ways to Counter Attacks

- Requiring **dual factor authentication** on all remote access (VPN, Citrix, Terminal Services, and webmail)
- Deployment of **application whitelisting technology** to critical assets (domain controllers, mail servers, file servers, etc.)
- **Network compartmentalization** of critical assets and data
- Deployment of **advanced malware detection/prevention** technology at the perimeter (web and email)
- Annual **penetration testing** of environments (internal and external networks, social engineering, and web applications)
- Searching for host and network-based **indicators of compromise** on a periodic basis
- Inventorying **service accounts** and resetting passwords on a periodic basis
- Blocking or requiring “click through” authentication when browsing to **uncategorized websites**

QUESTIONS?

Charles Carmakal

Managing Director

charles.carmakal@mandiant.com

864-735-7242