THE CYBER THREAT LANDSCAPE: NEW THEMES IN PREVENTION, DETECTION, RESPONSE

Kimberly Peretti
Partner, Alston & Bird, LLP
AGENDA

► Cyber Threat Landscape
  ► Nation States
  ► Organized criminal groups
  ► Hacktivists
  ► Lessons learned

► New Themes
  ► Response
  ► Detect
  ► Protect

► Take-aways
THREAT LANDSCAPE – NATION STATES
... the constant electronic theft of intellectual property that has silently occurred over the past several years has already caused significant harm to our national and economic security. Hackers have penetrated every kind of corporate network imaginable — from defense contractor databases containing important security information to business systems containing sensitive data and trade secrets. Cybercriminals are stealing American ideas, research, formulas, source code, trade secrets, classified government networks, email archives, negotiation plans, designs and blueprints on a massive scale.

What we have witnessed over the past five to six years has been nothing short of a historically unprecedented transfer of wealth — closely guarded national secrets (including those from classified government networks), source code, bug databases, email archives, negotiation plans and details for new oil and gas exploration, “fallen off the truck” in the ever-growing electronic archives of dogged adversaries. Operation Shady RAT, McAfee, August 2011.
NATION-STATE ATTACKS

Cyber Warfare

http://www.bankinfosecurity.com/hacktivists-suspend-ddos-attacks-a-5458?rf=2013-01-29-eb&elq=16d60e649ac743c3bd8642efdef64b87&elqCampaignId=5685.
THREAT LANDSCAPE – ORGANIZED CRIMINALS
Dirt Jumper DDoS Botnet Variants Continue to Proliferate

Friday, April 13, 2012

Researchers at Arbor Networks have identified so many varieties of the RustyKill distributed denial of service (DDoS) botnet that they have dubbed the variants collectively as the "Dirt Jumper family."

"Attacks from the Dirt Jumper family of bots continue to target victims all around the world in a robust manner and we will take a look at who is being attacked, although we cannot always determine the motive," writes Arbor Networks' Curt Wilson.

In denial of service attacks, generally a large amount of information is sent to a web server at such high frequency that it overwhelms the processing capacity or causes the system to shut down and reset altogether.

The proliferation of the Dirt Jumper botnets have spawned an underground economy based on DDoS attacks for hire, according to the research.

"While we have collected about 300 malware samples of the Dirt Jumper family, it is likely that other variants are available, as the binaries and back-end PHP for Dirt Jumper has leaked several times. This makes it easy for someone to make slight modifications to the PHP or Delphi binary code and attempt to re-sell the bot, use the bot for their own purposes, or start making money with their own commercial DDoS service," Wilson said.

"Dirt Jumper continues to evolve (version 5 appears to be the newest) and a variety of other associated bots packages have emerged over time to include Simple, September, Khan, Pandora, the DiBotNet and at least one private version of Dirt Jumper 5 that I am aware of," Wilson continued.


PROFILES OF CYBERCRIMINALS

http://www.nytimes.com/2010/11/14/magazine/14Hacker-t.html?pagewanted=all&_r=0
Anonymous, its security breaches, ...

The agents spent an hour and 40 minutes at Jordan’s house; other agents investigated a second home in New York; sources told Fox News that

Anonymous, its security breaches, ...

The agents spent an hour and 40 minutes at Jordan’s house; other agents investigated a second home in New York; sources told Fox News that...
LESSONS LEARNED

- Era of targeted intrusions
- Same methods (or modus operandi) occur time and time again
- Blending of methods, tactics, and techniques among groups
- Containment / eradication may take months not days
- Number of systems compromised may well reach into the hundreds
- Somewhere along the way, PII will probably come into play
RESPONSE
NEW THEMES: RESPONSE

- Enterprise impact investigations
- Crisis management
- Active Defense
ENTERPRISE IMPACT INVESTIGATIONS

► Three common breach response scenarios
► Inherent limitations
  ► Lack of privilege
  ► Incomplete understanding of scope of breach
ENTERPRISE IMPACT INVESTIGATIONS

- Hallmarks of an enterprise impact investigation
- Are enterprise impact investigations necessary? And, when?
What types of services may be relevant in a cyber response / data breach incident?

- Public relations services
- Intelligence gathering services
- Incident response support services
- Forensic investigation services
- Malware analysis services
- Network traffic monitoring services
- Data analysis services
- Breach notification support services

Not all of the services can be handled internally or even with one vendor.
CRISIS MANAGEMENT

Establish retainers/relationships up front
ACTIVE DEFENSE

Singapore's cybersecurity amendments opens questions on compliance

Summary: The government is proposing the word "cybersecurity" be included in the country's Computer Misuse Act. It will also harden the legislation to include pre-emptive actions.

In a bid to harden Singapore's cyberdefense, the government has proposed upgrades to its Computer Misuse Act.

http://www.zdnet.com/sg/singapores-cybersecurity-amendments-opens-questions-on-compliance-7000007565/


http://www.alstonprivacy.com/?entry=4793
DETECT
NEW THEMES - DETECT

- Preventative forensics
- “Big Data” forensics (detect/respond)
PREVENTATIVE FORENSICS

- Periodic scanning for breach indicators
  - Key systems
  - Assortment of endpoints
  - Updated list of indicators
- Component of cyber risk assessment
Training big data's eye on cybersecurity threats

Summary: The data explosion is upon us. Big data analytics is supposed to help us sift through it all. Can it also help keep enterprise hackers at bay? We talk to the founders of Seculert.

http://www.zdnet.com/training-big-datas-eye-on-cybersecurity-threats-700008357/
PROTECT
NEW THEMES: PROTECT

► Use of threat intelligence
► Threat modeling / assessment
THREAT INTELLIGENCE
THREAT INTELLIGENCE

► Use threat data points gathered in real-time from the criminal underground to analyze and understand
  ► The specific threat actors targeting your network
  ► The assets within your organization they are targeting
  ► The methods by which they are entering your networks/systems

► Aggregate/analyze this content in order to:
  ► Drive formation of a security strategy
  ► Determine security spending
  ► Implementation of, or changes to, security controls and capabilities

► Risk-based approach to security, not compliance-based
THREAT MODELING / ASSESSMENT

- Threat models/assessment
  - Understanding current defenses in place to protect against most likely threat vectors
  - Should be part of cyber risk assessment
FINAL THOUGHTS / LESSONS LEARNED
5 TIPS TO TAKE HOME

► Invest in information sharing
  ► Real-time mechanisms are the key to threat intelligence

► Don’t get caught in trap of narrowly-tailored investigations
  ► The sooner you uncover the scope, the better

► Use Big Data concepts to manage investigations
  ► The technology is there, use it

► Explore creative solutions in active defense space
  ► But this is especially an area to include counsel

► Hail to the Board
  ► Board involvement necessary in protect, detect, and respond
QUESTIONS?

Kimberly.peretti@alston.com
202.251.8118

For additional information, please see:
www.alstonprivacy.com
www.alstoncyber.com
www.alstonsecurity.com