The Cyber Threat

Organizational Lessons From The Front Lines

Bob Gourley, Partner, Cognitio
Nov 7, 2017

How we think.

The State of Cybersecurity Today

The Threat

A great deal is known about who is attacking and what their motivations are. By studying them we can build better defenses before attack and respond smarter during attack. Get the right info for strategic, operational and tactical decisions.

Adversaries Are:

Nations Crime Groups Extremists Hackers Insiders

Successful Attacks Are By Organizations

The Situation

Every sector of the economy and every government and every citizen is under almost constant attack. Most suffer ongoing infections with malware. Attackers get in fast and remain undetected for months. But risk can be reduced/mitigated.

Top Lessons Are:

Attackers are persistent, we must prepare for breach

Defenders Should Collaborate on Lessons

Unique Tech Factors

Governments, businesses, homes, aircraft, cars, roads, trains, ships, satellites, interconnected. But cyberspace is hard to observe. Well instrumented systems overseen by trained/experienced people are key to defense.

Tools To Consider:

Encryption ID Management 2FA Automated Patching

Ensure Tech is Independently Assessed

Your Action

Lead with understanding that cybersecurity is not just a tech function. Must have executive leadership and engagement by entire team. Ensure external verification and validation of strategy, policy, process and tech.

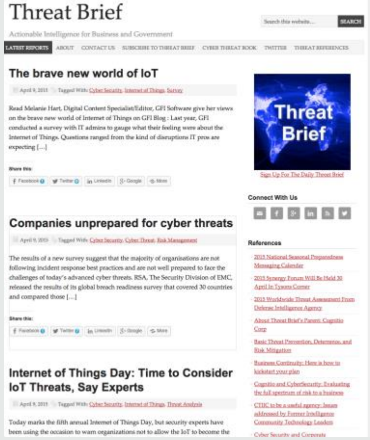
Top Actions:

Engage with ISACs, Collaborate with Peers, Study Threats

Victory Must Be Earned

About This Presentation

Based on two sources, our daily Threat Brief and our book on The Cyber Threat



Threat Brief

Actionable Intelligence for Business and Government

The brave new world of IoT

April 9, 2015 Tagged With: Cyber Security, Internet of Things, Survey

Read Melanie Hart, Digital Content Specialist/Editor, GFI Software give her views on the brave new world of Internet of Things on GFI Blog : Last year, GFI conducted a survey with IT admins to gauge what their feeling were about the Internet of Things. Questions ranged from the kind of disruptions IT pros are expecting […]

Companies unprepared for cyber threats

April 9, 2015 Tagged With: Cyber Security, Cyber Threat, Risk Management

The results of a new survey suggest that the majority of organisations are not following incident response best practices and are not well prepared to face the challenges of today's advanced cyber threats. RSA, The Security Division of EMC, released the results of its global breach readiness survey that covered 30 countries and compared those […]

Internet of Things Day: Time to Consider IoT Threats, Say Experts

April 9, 2015 Tagged With: Cyber Security, Internet of Things, Threat Analysis

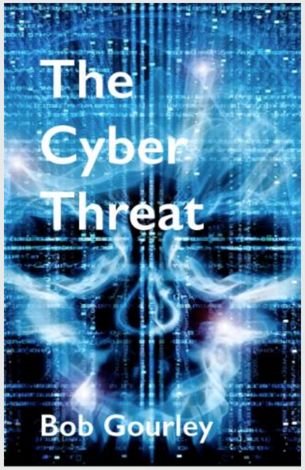
Today marks the fifth annual Internet of Things Day, but security experts have been using the occasion to warn organizations not to allow the IoT to become the

Sign Up For The Daily Threat Brief

Connect With Us

References

- 2015 National Seasonal Preparedness Messaging Calendar
- 2015 Synergy Forum Will Be Held 30 April In Tysons Corner
- 2015 Worldwide Threat Assessment From Defense Intelligence Agency
- About Threat Brief's Parent: Cognitio Corp
- Basic Threat Prevention, Deterrence, and Risk Mitigation
- Business Continuity: Here is how to kickstart your plan
- Cognitio and CyberSecurity: Evaluating the full spectrum of risk to a business
- CTIIC to be a useful agency: Issues addressed by Former Intelligence Community Technology Leaders
- Cyber Security and Corporate



ThreatBrief.com

TheCyberThreat.com

Both of these sources are meant for business leaders, not just security professionals

Some Discussion Topics

- What can study of human history tell us about the cyber threat?
- What can lessons from today’s fight tell us about tomorrow’s fight?
- Why does mind-expanding science fiction help us think about cyber defense?
- How can we all better protect our family’s private information and avoid cyber crime/fraud?

The Condensed History of the Cyber Threat

- Civil War: Both sides attacked, exploited, hacked
- 1998 Moonlight Maze: It takes a nation to fight a nation
- 2007 Estonia: Be ready to weather a storm
- 2008 Georgia: Expect cyber attacks timed to military ops
- 2008 Turkey Pipeline: Large cyber to physical attack
- 2011 Wikileaks: Know the human element. Know balance between info sharing and protection
- 2013 Mandiant Report: Cyber intel is strategic
- 2013 Snowden Leaks: Know the threat before it strikes
- 2013/14 Banks and Retail: Nothing stops this adversary
- 2014/15 Cars and Embedded IT: Threat actors will find a way
- 2015 Healthcare and Governments: No sector immune
- 2016: Turla Attacks: Telecom sector a target
- 2016: Shift to small and mid-sized businesses, supply chain, and home users

Today’s hackers are made of the same stuff as the famously persistent Hannibal, who did not give up till he got through the impassible firewall of the Alps

The Situation Today

- Everyone is under continuous attack
  - Personally
  - Enterprises
  - Manufacturing
  - Transportation
  - Telecom
- Everyone has ongoing infections with malware
- Attackers get in fast, but remain undetected for months
- New cloud and access control approaches provide opportunity to enhance security, if solutions engineered well

Hot Topics From The Daily Threat Brief

- The most famous attacks are the big ones (Equifax, Anthem, Y!, OPM, NSA, Target, Home Depot) but criminals prefer small and mid-sized businesses and individual users (you!)
- DDoS attacks large enough to take companies offline
- IoT is here... But little indication of IoT security solutions (I have studied every IoT security company I can find… Lots more room for innovation here)
- Cyber attacks against most sectors are growing and dangerous (but fastest growth at this time is in IoT in all sectors)
- Complex command and control infrastructures leverage unsuspecting companies and their servers/telecom
- Ransomware evolving/becoming harder to prevent/beat
- Phishing remains dominant path to organizations… exploits human traits of compassion and curiosity.
- Mobile device vulnerabilities: exploited to gain account info

Projecting These Trends Out To 2018

- The many attack vectors underway now will continue
  - Phishing will still be huge
  - Ransomware will keep evolving (so is traditional malware)
- Activists leveraging cyber attacks combined with media attacks
- Growth of IIoT Threats (will be disruptive of supply chain)
  - Reaper botnet is just the beginning
- All enterprises will need more automation of defenses, enhanced breach response plans and operational agility
- Great Trend: More awareness!

The Economist
The Pearl river delta: a special report
Hospitals of the future
Jacob Zuma must go
Parking, wrong on so many levels
Why computers will never be safe

Who is Attacking?

- Successful attacks are conducted by organizations: Groups of people acting together for a common purpose
- By studying those organizations and how they behave and what they want we can help deter their actions and mitigate some of their capabilities
- When under attack we can better defend
- When penetrated we can more quickly respond

The four categories of organizations: Nations, Criminals, Extremists, Hactivists (with Insiders potentially being one of any of those)

The Threat Actors

ACTOR	MOTIVE	TARGETS
Nation States	Economic or Military	IP or Infrastructure
Organized Crime	Financial Gain	IP, Banks, PoS
Terrorists / Extremists	Cause Support	Highly Visible Targets
Hackers / Hacktivists	Publicity, Watch it burn	Anything and Everything
Trusted Insiders	Revenge, Financial Gain	Your Data and/or Networks

Attack Patterns

METHOD	SUMMARY	LESSONS
Espionage Methods	Human-guided use of tools to find and extract information	Prioritize, classify, and protect data
Web Application Attacks	Breaking into web sites or applications	Don't host web sites on your network; use robust DMZs
Malicious Code	Viruses, worms, etc	Automatic detection and remediation
Exploit poor configuration	Take advantage of bad design	Understand your applications – alter default configurations
PoS Attacks	Financial transactions are always vulnerable	Ensure access to tactical threat intelligence; Red Teams

Bad Actors and Their Code

- Modern malware is designed to stay under the radar
  - Old anti-virus solutions do not work against new threats
  - Malware hops between media
  - Slow, hard to observe communications
  - Sandboxing, honeypots/nets not the entire solution
- Even sophisticated adversaries and modern malware can be detected
  - No adversary can be invisible
  - Well trained incident response teams find them
  - However, non-automated methods are overwhelmed and cannot scale
- Automation is key, including automating cyber intelligence

Foundational Work Has Been Done Enabling Automation

Discussion Topic: Kobayashi Maru

- Do you believe in no-win scenarios?
- Remember, people designed cyberspace
- We can design in better security
- You can chose to operate your home technology in more secure ways

Some Review

- **Adversaries Will Keep Coming:** History and current operations show criminals are going to keep trying. They will change
- **Malware, Especially Ransomware, is evolving:** It is serious today, but will be more serious tomorrow. Get ready now.
- **You cannot beat the bad guys alone/It takes teams to beat teams:** Leverage the power of teams for your defense. Security professionals, law enforcement, cloud service providers, SAE, Auto-ISAC
- **You can have great influence over your home systems and how they are used:** Like Kirk and the Kobayashi Maru, you don’t have to lose.
- **Be Prepared To Be Surprised:** Another big lesson from both history and current operations. You will be surprised. Have an incident response plan.

What Can We Do About It?

- **Take Command Of The Discussion and Improve Understanding:** Use common taxonomy for all internal and external communications (NIST Cybersecurity Framework is good).
- **Engineer for Success:** See SAE 3061 Guidebook for Cyber-Physical Vehicle Systems.
- **Contribute to Community:** What are best practices for cybersecurity, including cybersecurity fail-safes? What are best practices for sharing designs?
- **Design for Containment:** Early detection and rapid incident response will be aided if systems are designed to contain adversaries. Containment of attacks is especially important in malicious code.
- **Assess and Understand:** Know what data, comms and capabilities contribute to the overall vehicle system. Improve design and build in monitoring plus ability to update.
- **Enhance Defenses (but prepare for breach):** The adversary in cyberspace is continuing to innovate, which means we must continue to review our defenses and modernize. Even with this continual defense, history proves that the adversaries eventually get in.

What Can We Do About It?

- **Ensure Availability and Backup:** Every critical system must have appropriate level of availability and a backup, and recovery methods must be defined and tested.
- **Coordinate Early:** Work with those that are critical to preventing and responding to attacks. For example, the FBI, the US CERT, and the appropriate ISAC (Auto-ISAC for auto sector). Build bonds of trust before an incident.
- **Leverage Experience of Others:** No organization can match the technical talent of the modern cyber criminal or nation. This requires seasoned professionals who constantly focus on learning threat tactics and mitigation strategies. Engage with SAE. Engage with the security research community (Hackers!)
- **Automate Defenses and Enhance Monitoring:** Here too external help is almost always the right path forward.
- **Training for employees:** this includes awareness at work and at home. Breaches there can impact vehicle solutions. Employees are first line of defense and need to know in clear language what to do and what to report.

But What About Your Personal IT?

Our short list of tips follows

How You Operate Your Home IT

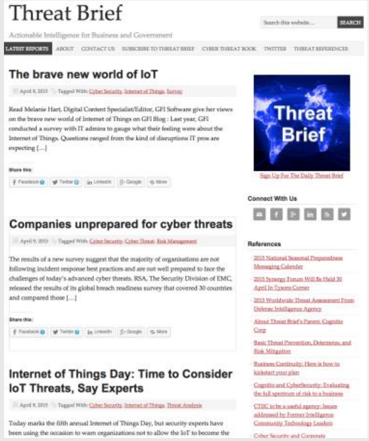
- **Use The Cloud:** Don’t use your ISP’s email. Use Google Apps or other large online service that dedicates resources to security.
- **Keep all your systems patched, always:** You are the fortunate ones. You can afford modern IT and can afford to keep it patched.
- **Anti-malware solutions are all flawed, but you need them!:** Mac users: Sophos or Malwarebytes. PC users: Symantec or Kaspersky.
- **Use a password manager:** Use Dashlane. Follow its advice.
- **Use managed DNS:** From Verisign, OpenDNS, or Google.
- **Backup:** When your defenses fail and ransomware hits, you will be glad you backed up. Carbonite is a popular backup for home users.
- **Give to Get:** Help your neighbors, friends, family become more secure and it will help us all out.

Concluding Recommendations

Continually Learn!

Know and Improve Your Policies!

Communicate!



Threat Brief

Search this website... SEARCH

Actionable Intelligence for Business and Government

LATEST REPORTS ABOUT CONTACT US SUBSCRIBE TO THREAT BRIEF CYBER THREAT BOOK TWITTER THREAT REFERENCES

The brave new world of IoT

April 9, 2015 Tagged With: Cyber Security, Internet of Things, Survey

Read Melanie Hart, Digital Content Specialist/Editor, GFI Software give her views on the brave new world of Internet of Things on GFI Blog : Last year, GFI conducted a survey with IT admins to gauge what their feeling were about the Internet of Things. Questions ranged from the kind of disruptions IT pros are expecting […]

Share this:

Facebook Twitter LinkedIn Google More

Companies unprepared for cyber threats

April 9, 2015 Tagged With: Cyber Security, Cyber Threat, Risk Management

The results of a new survey suggest that the majority of organisations are not following incident response best practices and are not well prepared to face the challenges of today's advanced cyber threats. RSA, The Security Division of EMC, released the results of its global breach readiness survey that covered 30 countries and compared those […]

Share this:

Facebook Twitter LinkedIn Google More

Internet of Things Day: Time to Consider IoT Threats, Say Experts

April 9, 2015 Tagged With: Cyber Security, Internet of Things, Threat Analysis

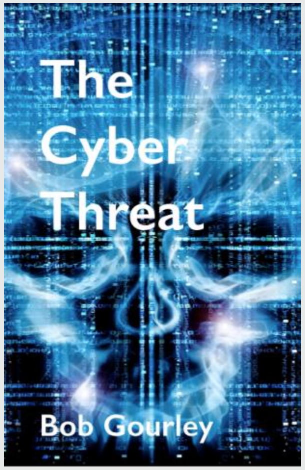
Today marks the fifth annual Internet of Things Day, but security experts have been using the occasion to warn organizations not to allow the IoT to become the

Sign Up For The Daily Threat Brief

Connect With Us

References

- 2015 National Seasonal Preparedness Messaging Calendar
- 2015 Synergy Forum Will Be Held 30 April In Tysons Corner
- 2015 Worldwide Threat Assessment From Defense Intelligence Agency
- About Threat Brief's Parent: Cognitio Corp
- Basic Threat Prevention, Deterrence, and Risk Mitigation
- Business Continuity: Here is how to kickstart your plan
- Cognitio and CyberSecurity: Evaluating the full spectrum of risk to a business
- CTIIC to be a useful agency: Issues addressed by Former Intelligence Community Technology Leaders
- Cyber Security and Corporate



ThreatBrief.com

TheCyberThreat.com

Bob.gourley@cognitiocorp.com

About Cognitio

We Do Three Things

Cognitio is a strategic consulting and engineering firm led by a team of former senior technology executives from the U.S. Intelligence Community and financial sector.

We have a track record of safeguarding some of the nation’s greatest secrets, equipping U.S. leadership with actionable intelligence that helps protect lives and driving technology innovation that kept key government agencies generations ahead.

Cognitio enables companies to effectively manage technology, maximize technology investments, and reduce overall institutional risk.

Cyber Security

We provide cyber assessment, CISO-as-a-Service, action plans, awareness, remediation and containment strategies. Our process, the Cyber360, includes best practices from government and industry.

Innovation

Continued innovation is required for market success. Innovation requires well thought out action plans informed by knowledge of both legacy and new technologies.

Data Analytics

We know the “so-what” of data, it is there to enhance your ability to achieve your business objectives. And we know the infrastructure and applications required to let you take advantage of your data.

CognitioCorp.com

Current Engagements

- Independent assessments of security posture leveraging best practices and our Cyber360 framework
- Campaign plans and technology assessments enabling optimization of security spend
- Evaluation of and exercising of incident response plans
- Cyber threat intelligence architecture, data source and process reviews
- Cyber threat training and exercises for the workforce
- Independent verification and validation of compliance
- CISO as a Service: Executive leadership to lower digital risk and increase speed of innovation

Bob Gourley

bob.gourley@cognitiocorp.com

How we think.