https://www.guardsight.com/

Founded in 2009, GuardSight is a cybersecurity services company that helps businesses of all sizes safeguard their digital assets and reputations against online threats.

"We fight bad guys on the internet!"

John McGloughlin, CISSP

Founder & CEO GuardSight, Inc.

johnmac@guardsight.com

CYBERSECURITY: A General Discussion

(my pgp key) → http://pgp.mit.edu johnmac@guardsight.com | https://www.linkedin.com/in/mcgloughlin ← (about me)

HISTORY: CYBERSECURITY & CYBERCRIME

1900-1949

- '03 - Magician hacks Marconi's secure wireless telegraph ("hacking" wasn't actually coined until '55 @ an MIT model railroad club)
- '32 - Enigma machine code broken by Polish cryptologists
- **'39 - Turing co-develops the Bombe making the Enigma machine vulnerable to *brute force attacks***

1950-1979

- '57 - A blind boy (7 yrs. old) discovers that whistling the fourth E > middle C interferes with AT&T's telephone systems (phreaking)
- '63 - Hackers tie up phone lines between Harvard and MIT and make long-distance calls charged to a local radar installation (1st malicious)
- **'71 - Rosenbaum/Esquire publishes "*Secrets of the Little Blue Box*" relies on accounts from Draper (Captain Crunch) and a toy whistle**
- '72 - Draper arrested (toll fraud - 5yrs prob) - catalyst for Wozniak meeting and connection - Jobs & Wozniak sold phone-phreaking tools
- '79 - Mitnick (16 yrs. old) breaks into the DEC ARK system used for developing their RSTS/E operating system software (social engineering)

1980-1999

- '81 - The 414s break into 60 computers at multiple institutions including the Los Alamos National Laboratory (cover of Newsweek)
- **'83 - Release of the movie WarGames introduces the wider public to hacking (the WOPR discovers the concept of Mutually Assured Destruction)**
- '86 - Congress passes the CFAA (18 U.S.C 1030) making it a crime to break into computers (amended '89, '94, '96, '01, '02, '08, '15)
- '88 - Morris introduces a worm that alters 6k ARPANET computers (booted from Cornell / convicted of violating CFAA) / CERT created by DARPA
- '96 - Hackers alter the web sites of the DOJ, CIA, and US Air Force / RIAA begins cracking down on file sharing
- '98 - The US NIPC is established to fight sabotage of infrastructure (transferred to DHS in 2003, disbanded and now the NIPP concern)
- '99 - A plethora of high profile malware impacts millions of computers and causes > $100M in damages (Melissa, Chernobyl, Thursday, Bubble Boy)

GuardSight

HISTORY: CYBERSECURITY & CYBERCRIME

2000-2009

- ‘01 - Code Red worm infects > 350k web servers (MS01-033) / Sklyarov arrested at DEF CON - 1st charged w/violating DMCA
- ‘02 - ISC2 reports 10k CISSP certified worldwide (there are now > 70k worldwide)
- ‘03 - SQL Slammer worm released infecting 75,000 victims within 10 minutes / Hacktivist group Anonymous is formed
- ‘06 - Ancheta receives a 57mo sentence / Moore & Pena featured on America's Most Wanted / Turkish hacker compromises > 22k websites
- ‘07 - FBI BotRoast discovers > 1M botnet victims / Spear phishing at office of US Secretary Of Defense steals sensitive defense information
- ‘09 - Conficker worm infects 15M government, business, home computers in over 190 countries

2010-2018

- ‘10 - Google publicly reveals Operation Aurora - theft of intellectual property by Chinese APT group / Stuxnet disables Iranian nuclear facilities
- ‘11 - 77M accounts impacted from hack of Sony’s PlayStation network / Sesame Street hacked (porn streamed for 22 mins) / LulzSec formed
- ‘12 - 6M accounts impacted by LinkedIn hack / Marriott extorted by Nemeth / Saudi Aramco crippled by Cutting Sword of Justice cyber warfare
- ‘13 - 40M debit and credit cards exposed in Target breach ($252M losses) / 65M impacted from hack of social networking site Tumblr
- ‘14 - $460M stolen from bitcoin exchange Mt. Gox - (bankruptcy) / Sony Pictures severely wounded by Guardian of Peace attack
- ‘15 - 21.5m Americans impacted by attack on US OPM / Ashley Madison extramarital affair website hacked / Ukraine power grid hacked (SCADA ICS)
- ‘16 - $100M lost in Bangladesh bank cyber heist / Wikileaks publishes DNC email messages / Dyn DDOS attack - Mirai botnet (IOT devices)
- ‘17 - 10k orgs impacted by WannaCry in 150 countries / 140M people harmed by Equifax breach / 57M hit by Uber breach / HBO & Netflix content stolen
- ‘18 - Atlanta disrupted for 1wk - ransomware (airport wifi shutdown) / Amazon DNS traffic redirected to Russia to steal cryptocurrency

STATISTICS: CYBERSECURITY PAIN IS REAL

- 73% of cyber compromise are *financially motivated* (27% espionage)
- $57B-$109B estimated cost of cybercrime to the U.S. economy in 2016
- $600B estimated global cost of cybercrime in 2017
- 230k new malware variants / 4k ransomware attacks globally every day
- 66% of malware is installed via *email* attachment
- $3B in losses were caused by BEC in the US between 2014-2017
- 43% of *phishing* campaigns targeted SMB in 2016 (18% in 2011)
- 14% of SMB rate their ability to handle cyber attacks as *highly effective*
- 60% of SMB go *out of business* within 6 months of a serious cyber compromise
- $1.9M average cost for breaches <10k records ($6.3M >50k records) in 2017
- 75% of cyber compromise perpetrated by *outsiders* (25% by insiders)
- 92% of *manufacturers* cite cyber concerns in their 2015-2016 SEC disclosures
- 72% of US utilities (power, water, sewer) cite cybersecurity as the top concern

GuardSight

THREAT ACTORS: ATTRIBUTION

Outsiders (Organized)

- Terrorists
  - Combatants
  - Physical / Psychological
- Hacktivists
  - Mobilizers
  - Political / Ideology / Idealism
- Nation States
  - Government Agencies
  - Recon / Sabotage / IP Theft
- Criminal Enterprises
  - Hierarchical Malevolents
  - Robbery / Fraud / Prostitution / Narcotics
- Robots
  - (d) All of the above

Outsiders (Non-Organized)

- Hackers
  - Black Hats
    - Explorers
    - Trespassers
    - Malicious Intruders
  - White Hats
    - Explorers
    - Trespassers
    - Responsible Disclosure
- Amatuers
  - Script Kiddies

Insiders

- Thieves
- Sponsored Agents
- 3rd Party Suppliers
- Disaffected Employees
- Improper Asset Protection

Nation States
- *APT-"n" (CN,RU,...)*
- *Bronze Union (CN)*
- *Cobalt Trinity (IR)*
- *Iron Twilight (RU)*
- *Lazarus Group (KP)*
- *Gold Skyline (NG)*

Crime Syndicates
- *FIN7*
- *ShadowCrew*

Hacktivists
- *Anonymous*
- *LulzSec*
- *WikiLeaks*

Botnets
- *Conficker*
- *Gameover Zeus*
- *Satori*
- *Mirai*

Dark Web Marketplaces
- *Olympus Market*
- *DutchDrugz*

GuardSight

THREAT ACTORS: SPECIFIC INTENT

- Identity Resources (***Impersonate***)
  - PII
  - PHI
  - Credentials
- Intellectual Resources (***Dominate***)
  - Brand
  - Property
  - Knowledge
- Physical Resources (***Perpetuate***)
  - Energy
  - Strength
  - Persistence
- Logical Resources (***Violate***)
  - Speech
  - Reputation
  - Communication

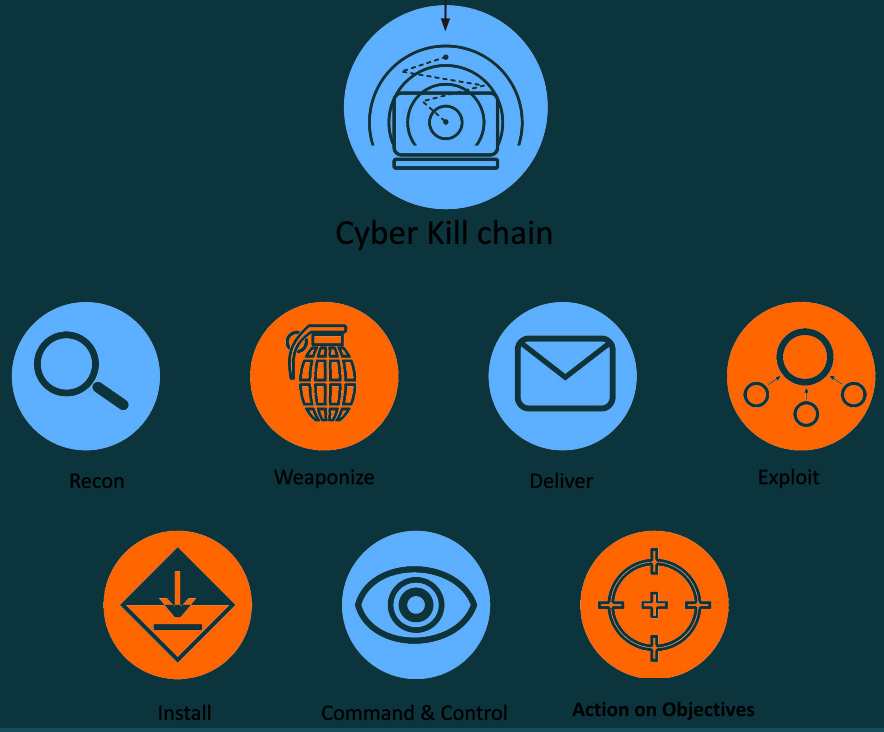
Objectives

- *Profit*
- *Wealth*
- *Assets*
- *Prestige*
- *Warfare*
- *Self-Defense*
- *Espionage*
- *Political Mobilization*
- *Theological Mobilization*
- *Ideal[ogy / ism]*
- *Competition Elimination*
- *Living Off The Land*
- *Employment*
- *Entrapment*
- *Extortion*
- *Evidence Destruction*

GuardSight

THREAT ACTORS: TTP

What They Want	*How They Plan To Get It*	*Evidence They Leave Behind*
Objectives	**TTP**	IOC



Techniques

- *Phishing*
- *Drive-by Downloads*
- *Ransomware*
- *Access Violations*
- *Vulnerability Exploits*
- *Configuration Exploits*
- *Process Injection*
- *Rootkits*
- *Web Shells*
- *Credential Harvesting*
- *Crypto Miners*
- *API Hooking*
- *Fileless Malware*
- *DLL Hijacking*
- *Registry Modifications*
- *Automated Exfil*
- *Task Scheduling*

GuardSight

DETECT AND RESPOND: TTP

~~RUN~~ ~~HIDE~~ **FIGHT!**

- Implement multi-factor authentication
- **Reduce the attack surface**
- Enhance and enrich logging (access/authorization)
- **Routinely backup critical assets**
- Remediate asset vulnerabilities (patch!) and configuration defects
- **Deploy and audit security controls (SCAP)**
- Segment critical assets
- **Deploy endpoint protection, detection, response technologies**
- Automate detection, inspections, and patrols (threat hunting)
- **Hire qualified, competent, passionate people**
- Create a cybersecurity aware culture & train employees
- **Reference NIST Cybersecurity Framework & NIST-SP-800**

- Legislation (CFAA, DMCA, HIPAA, GLBA, FISMA, GDPR, Breach Notification Laws)
- Compliance / Frameworks (PCI, SOC2, ISO/IEC 27001, NIST-SP-800, NIST-CSF)
- Insurance (> $3 billion in cybersecurity insurance premiums sold in 2017)

Techniques

- *Inventory*
- *Detect*
- *Deny*
- *Disrupt*
- *Deceive*
- *Degrade*
- *Destroy*

Response

- *Prepare*
- *Assess & Rate*
- *Memorialize*
- *Contain*
- *Remediate & Recover*
- *After-Action Report*
- *Notify External Entities*
- *Engage 3rd Party Pros*

GuardSight