Hacking Team

Jump to navigation Jump to search

HackingTeam

Industry	Information technology
Founded	2003
Founders	David Vincenzetti, Valeriano Bedeschi
Headquarters	Milan, Italy
Products	Software
Website	HackingTeam.it

HackingTeam was a Milan-based information technology company that sold offensive intrusion and surveillance capabilities to governments, law enforcement agencies and corporations.[1] Its "*Remote Control Systems*" enable governments and corporations to monitor the communications of internet users, decipher their encrypted files and emails, record Skype and other Voice over IP communications, and remotely activate microphones and camera on target computers.[2] The company has been criticized for providing these capabilities to governments with poor human rights records,[3] though HackingTeam states that they have the ability to disable their software if it is used unethically.[4][5] The Italian government has restricted their licence to do business with countries outside Europe.[6]

HackingTeam employs around 40 people in its Italian office, and has subsidiary branches in Annapolis, Washington, D.C., and Singapore.[7] Its products are in use in dozens of countries across six continents.[8]

Company foundation

HackingTeam was founded in 2003 by Italian entrepreneurs Vincenzetti and Valeriano Bedeschi. In 2007 the company was invested by two Italian VC: Fondo Next and Innogest.[9]

The Milan police department learned of the company. Hoping to use its tool to spy on Italian citizens and listen to their Skype calls, the police contacted Vincenzetti and asked him to help.[10] HackingTeam became "the first sellers of commercial hacking software to the police".

According to former employee Byamukama Robinhood, the company began as security services provider, offering penetration testing, auditing and other defensive capabilities to clients.[11] Byamukama states that as malware and other offensive capabilities were developed and accounted for a larger percentage of revenues, the organization pivoted in a more offensive direction and became increasingly compartmentalized. Byamukama claims fellow employees working on aspects of the same platform – for example, Android exploits and payloads – would not communicate with one another, possibly leading to tensions and strife within the organization.[11]

In February 2014, a report from Citizen Lab identified the organisation to be using hosting services from Linode, Telecom Italia, Rackspace, NOC4Hosts and bullet proof hosting company Santrex.[12]

On 5 July 2015 the company suffered a major data breach of customer data, software code, internal documents and e-mails. (*See: § 2015 data breach*)

On 2 April 2019 HackingTeam was acquired by InTheCyber Group to create Memento Labs [13]

Products and capabilities

Hacking Team enables clients to perform remote monitoring functions against citizens via their RCS (remote control systems), including their Da Vinci and Galileo platforms:[1]

- Covert collection of emails, text message, phone call history and address books
- Keystroke logging
- Uncover search history data and take screenshots
- Record audio from phone calls

- Capture audio and video stream from device memory to bypass cryptography of Skype sessions[14]
- Use microphones on device to collect ambient background noise and conversations

- Activate phone or computer cameras
- Hijack telephone GPS systems to monitor target's location
- Infect target computer's UEFI BIOS firmware with a rootkit[15]
- Extract WiFi passwords[16]
- Exfiltrate Bitcoin and other cryptocurrency wallet files to collect data on local accounts, contacts and transaction histories[17]

HackingTeam uses advanced techniques to avoid draining cell phone batteries, which could potentially raise suspicions, and other methods to avoid detection.[18][19]

The malware has payloads for Android,[16] BlackBerry, Apple iOS, Linux, Mac OS X, Symbian, as well as Microsoft Windows, Windows Mobile and Windows Phone class of operating systems.[20]

RCS is a management platform that allows operators to remotely deploy exploits and payloads against targeted systems, remotely manage devices once compromised, and exfiltrate data for remote analysis.

Controversies

Use by repressive governments

HackingTeam has been criticized for selling its products and services to governments with poor human rights records, including Sudan, Bahrain, Venezuela, and Saudi Arabia.[21]

In June 2014, a United Nations panel monitoring the implementation of sanctions on Sudan requested information from HackingTeam about their alleged sales of software to the country in contravention of United Nations weapons export bans to Sudan. Documents leaked in the 2015 data breach of HackingTeam revealed the organization sold Sudanese National Intelligence and Security Service access to their "Remote Control System" software in 2012 for 960,000 Euros.[21]

In response to the United Nations panel, the company responded in January 2015 that they were not currently selling to Sudan. In a follow-up exchange, HackingTeam asserted that their product was not controlled as a weapon, and so the request was beyond the scope of the panel. There was no need for them to disclose previous sales, which they considered confidential business information.[21]

The U.N. disagreed. "The view of the panel is that as such software is ideally suited to support military electronic intelligence (ELINT) operations it may potentially fall under the category of 'military ... equipment' or 'assistance' related to prohibited items," the secretary wrote in March. "Thus its potential use in targeting any of the belligerents in the Darfur conflict is of interest to the Panel."[21][22]

In the fall of 2014, the Italian government abruptly froze all of HackingTeam's exports, citing human rights concerns. After lobbying Italian officials, the company temporarily won back the right to sell its products abroad.[21]

2015 data breach

On July 5, 2015, the Twitter account of the company was compromised by an unknown individual who published an announcement of a data breach against HackingTeam's computer systems. The initial message read, "*Since we have nothing to hide, we're publishing all our e-mails, files, and source code ...*" and provided links to over 400 gigabytes of data, including alleged internal e-mails, invoices, and source code; which were leaked via BitTorrent and Mega.[23] An announcement of the data breach, including a link to the bittorrent seed, was retweeted by WikiLeaks and by many others through social media.[24][25]

The material was voluminous and early analysis appeared to reveal that HackingTeam had invoiced the Lebanese Army[26] and Sudan and that spy tools were also sold to Bahrain and Kazakhstan.[25] HackingTeam had previously claimed they had never done business with Sudan.[27]

The leaked data revealed a zero-day cross-platform Flash exploit (CVE number: CVE-2015-5119.[28] The dump included a demo of this exploit by opening Calculator from a test webpage.[29][30][31] Adobe patched the hole on July 8, 2015.[32] Another vulnerability involving Adobe was revealed in the dumps, which took advantage of a buffer overflow attack on an Adobe Open Type Manager DLL included with Microsoft Windows. The DLL is run in kernel mode, so the attack could perform privilege escalation to bypass the sandbox.[33]

Also revealed in leaked data was HackingTeam employees' use of weak passwords, including 'P4ssword', 'wolverine', and 'universo'.[34]

After a few hours without response from HackingTeam, member Christian Pozzi tweeted the company was working closely with police and "*what the attackers are claiming regarding our company is not true.*"[35][36] He also claimed the leaked archive "contains a virus" and that it constituted "false info".[37] Shortly after these tweets, Pozzi's Twitter account itself was apparently compromised.[38]

Responsibility for this attack was claimed by the hacker known as "Phineas Fisher" (or Phisher) on Twitter.[39] Phineas has previously attacked spyware firm Gamma International, who produce malware, such as FinFisher, for governments and corporations.[40] In 2016, Phineas published details of the attack, in Spanish and English, as a "how-to" for others, and explained the motivations behind the attack.[41]

The internal documents revealed details of HackingTeam's contracts with repressive governments.[42] In 2016, the Italian government again revoked the company's license to sell spyware outside of Europe without special permission.[6][43]

Use by Mexican drug cartels

Corrupt Mexican officials have helped drug cartels obtain state-of-the-art spyware (including Hacking Team spyware). The software has been used to target and intimidate Mexican journalists by drug cartels and cartel-entwined government actors.[44]

Customer list

HackingTeam's clientele include not just governments, but also corporate clients such as Barclays and British Telecom (BT) of the United Kingdom, as well as Deutsche Bank of Germany.[1]

A full list of HackingTeam's customers were leaked in the 2015 breach. Disclosed documents show HackingTeam had 70 current customers, mostly military, police, federal and provincial governments. The total company revenues disclosed exceeded 40 million Euros.[45][46][47][48][49][50]

On Sep 8, 2021,SentinelLABS released a research report about a Turkish threat actor EGoManiac,that used Remote Control System (RCS), software from the Italian infosec firm Hacking Team,which was operated between 2010 and 2016 and campaign run by Turkish TV journalists at OdaTV for spying Turkish police.[51]

Customer	Country	Area	Agency	Year of first sale	Annual maintenance fees	Total client revenues
Polizia Postale e delle Comunicazioni[52]	Italy	Europe	LEA	2004	€100,000	€808,833
Centro Nacional de Inteligencia[53]	Spain	Europe	Intelligence	2006	€52,000	€538,000
Infocomm Development Authority of Singapore	Singapore	APAC	Intelligence	2008	€89,000	€1,209,967
Information Office	Hungary	Europe	Intelligence	2008	€41,000	€885,000
CSDN	Morocco	MEA	Intelligence	2009	€140,000	€1,936,050
UPDF (Uganda Peoples Defense Force), ISO (Internal Security Organization), Office of the President	Uganda	Africa	Intelligence	2015	€731,000	€920,197
Italy - DA - Rental	Italy	Europe	Other	2009	€50,000	€628,250
Malaysian Anti-Corruption Commission	Malaysia	APAC	Intelligence	2009	€77,000	€789,123
PCM	Italy	Europe	Intelligence	2009	€90,000	€764,297
SSNS - Ungheria	Hungary	Europe	Intelligence	2009	€64,000	€1,011,000
CC - Italy	Italy	Europe	LEA	2010	€50,000	€497,349
Al Mukhabarat Al A'amah	Saudi Arabia	MEA	Intelligence	2010	€45,000	€600,000
IR Authorities (Condor)	Luxembourg	Europe	Other	2010	€45,000	€446,000

La Dependencia y/o CISEN[54]	Mexico	LATAM	Intelligence	2010	€130,000	€1,390,000
UZC[55]	Czech Republic	Europe	LEA	2010	€55,000	€689,779
Egypt - MOD[55]	Egypt	MEA	Other	2011	€70,000	€598,000
Federal Bureau of Investigation[56]	USA	North America	LEA	2011	€100,000	€697,710
Oman - Intelligence	Oman	MEA	Intelligence	2011	€30,000	€500,000
President Security[57][58]	Panama	LATAM	Intelligence	2011	€110,000	€750,000
Turkish National Police	Turkey	Europe	LEA	2011	€45,000	€440,000
UAE - MOI	UAE	MEA	LEA	2011	€90,000	€634,500
National Security Service[55]	Uzbekistan	Europe	Intelligence	2011	€50,000	€917,038
Department of Defense[56]	USA	North America	LEA	2011		€190,000
Bayelsa State Government	Nigeria	MEA	Intelligence	2012	€75,000	€450,000
Estado de Mexico	Mexico	LATAM	LEA	2012	€120,000	€783,000
Information Network Security Agency	Ethiopia	MEA	Intelligence	2012	€80,000	€750,000
State security (Falcon)	Luxemburg	Europe	Other	2012	€38,000	€316,000
Italy - DA - Rental	Italy	Europe	Other	2012	€60,000	€496,000
MAL - MI	Malaysia	APAC	Intelligence	2012	€77,000	€552,000
Direction générale de la surveillance du territoire	Morocco	MEA	Intelligence	2012	€160,000	€1,237,500
National Intelligence and Security Service[55]	Sudan	MEA	Intelligence	2012	€76,000	€960,000
Russia - KVANT[59]	Russia	Europe	Intelligence	2012	€72,000	€451,017

Saudi - GID	Saudi	MEA	LEA	2012	€114,000	€1,201,000
SIS of National Security Committee of Kazakhstan[55]	Kazakhstan	Europe	Intelligence	2012	€140,000	€1,012,500
The 5163 Army Division (Alias of South Korean National Intelligence Service)[55][60][61]	S. Korea	APAC	Other	2012	€67,000	€686,400
UAE - Intelligence	UAE	MEA	Other	2012	€150,000	€1,200,000
Central Intelligence Agency[62]	USA	North America	Intelligence	2011		
Drug Enforcement Administration[56][63]	USA	North America	Other	2012	€70,000	€567,984
Central Anticorruption Bureau	Poland	Europe	LEA	2012	€35,000	€249,200
MOD Saudi	Saudi	MEA	Other	2013	€220,000	€1,108,687
PMO	Malaysia	APAC	Intelligence	2013	€64,500	€520,000
Estado de Queretaro	Mexico	LATAM	LEA	2013	€48,000	€234,500
National Security Agency[55]	Azerbaijan	Europe	Intelligence	2013	€32,000	€349,000
Gobierno de Puebla	Mexico	LATAM	Other	2013	€64,000	€428,835
Gobierno de Campeche	Mexico	LATAM	Other	2013	€78,000	€386,296
AC Mongolia	Mongolia	APAC	Intelligence	2013	€100,000	€799,000
Dept. of Correction Thai Police	Thailand	APAC	LEA	2013	€52,000	€286,482
National Intelligence Secretariat[64]	Ecuador	LATAM	LEA	2013	€75,000	€535,000
Police Intelligence Directorate	Colombia	LATAM	LEA	2013	€35,000	€335,000

Guardia di Finanza	Italy	Europe	LEA	2013	€80,000	€400,000
Intelligence[65]	Cyprus	Europe	LEA	2013	€40,000	€375,625
MidWorld[66]	Bahrain	MEA	Intelligence	2013		€210,000
Mexico - PEMEX	Mexico	LATAM	LEA	2013		€321,120
Malysia K	Malaysia	APAC	LEA	2013		€0
Honduras	Honduras	LATAM	LEA	2014		€355,000
Mex Taumalipas	Mexico	LATAM		2014		€322,900
Secretaría de Planeación y Finanzas	Mexico	LATAM	LEA	2014	€91,000	€371,035
AREA	Italia	Europe		2014		€430,000
Mexico Yucatán	Mexico	LATAM	LEA	2014		€401,788
Mexico Durango	Mexico	LATAM	LEA	2014		€421,397
Investigations Police of Chile	Chile	LATAM	LEA	2014		€2,289,155
Jalisco Mexico	Mexico	LATAM	LEA	2014		€748,003
Royal Thai Army	Thailand	APAC	LEA	2014		€360,000
Vietnam GD5	Vietnam	APAC		2014		€281,170
Kantonspolizei Zürich	Switzerland	Europe	LEA	2014		€486,500
Vietnam GD1	Vietnam	APAC	LEA	2015		€543,810
Egypt TRD GNSE	Egypt	MEA	LEA	2015		€137,500
Lebanese Army	Lebanon	MEA	LEA	2015		
Federal Police Department	Brazil	LATAM	LEA	2015		
National Anticorruption Directorate	Romania	DNA	Intelligence	2015		
State Informative Service[67]	Albania	Europe	SHIK	2015		

Danish National Police[68]	Denmark	Europe	2015	€570,000

See also

- FinFisher
- MiniPanzer and MegaPanzer

References

1. ^ **a** **b** **c** *Batey, Angus (24 November 2011). "The spies behind your screen". The Telegraph. Retrieved 26 July 2015.*
2. **^** *"Enemies of the Internet: HackingTeam". Reporters Without Borders. Archived from the original on 29 April 2014. Retrieved 24 April 2014.*
3. **^** *Marczak, Bill; Gaurnieri, Claudio; Marquis-Boire, Morgan; Scott-Railton, John (17 February 2014). "Mapping HackingTeam's "Untraceable" Spyware". Citizen Lab. Archived from the original on 20 February 2014.*
4. **^** *Kopfstein, Janus (10 March 2014). "Hackers Without Borders". The New Yorker. Retrieved 24 April 2014.*
5. **^** *Marquis-Boire, Morgan; Gaurnieri, Claudio; Scott-Railton, John; Kleemola, Katie (24 June 2014). "Police Story: HackingTeam's Government Surveillance Malware". Citizen Lab. University of Toronto. Archived from the original on 25 June 2014. Retrieved 3 August 2014.*
6. ^ **a** **b** *Zorabedian, John (8 April 2016). "HackingTeam loses global license to sell spyware". Naked Security. Retrieved 15 May 2016.*
7. **^** *Human Rights Watch* (25 March 2014). "They Know Everything We Do". Retrieved 1 August 2015.
8. **^** *Jeffries, Adrianne (13 September 2013). "Meet HackingTeam, the company that helps the police hack you". The Verge. Retrieved 21 April 2014.*
9. **^** *Jeffries, Adrianne (13 September 2013). "Meet Hacking Team, the company that helps the police hack you". The Verge. Retrieved 20 August 2021.*
10. ^ **a** **b** Farivar, Cyrus (20 July 2015) HackingTeam goes to war against former employees, suspects some helped hackers. *Ars Technica*. Retrieved 26 July 2015.
11. **^** *"HackingTeam's US Nexus". 28 February 2014. Retrieved 2 August 2015.*
12. **^** *Stecklow, Steve; Sonne, Paul; Bradley, Matt (1 June 2011). "Mideast Uses Western Tools to Battle the Skype Rebellion". The Wall Street Journal. Retrieved 26 July 2015.*
13. **^** *Lin, Philippe (13 July 2015). "HackingTeam Uses UEFI BIOS Rootkit to Keep RCS 9 Agent in Target Systems". TrendLabs Security Intelligence Blog. Trend Micro. Retrieved 26 July 2015.*
14. **^** *Schneier, Bruce. "More on HackingTeam's Government Spying Software".*
15. **^** Guarnieri, Claudio; Marquis-Boire, Morgan (13 January 2014). "To Protect And Infect: The militarization of the Internet". At the 30th Chaos Communications Congress – "30C3". (Video or Audio). Chaos Computer Club. Retrieved 15 August 2015.

16. ^ a b c d e Hay Newman, Lily (7 July 2015). "A Detailed Look at HackingTeam's Emails About Its Repressive Clients". The Intercept. Retrieved 15 May 2016.
17. ^ Knibbs, Kate (8 July 2015). "HackingTeam's Lame Excuse for Selling Digital Weapons to Sudan". Gizmodo. Retrieved 15 May 2016.
18. ^ "Hacked Team (@hackingteam)". Archived from the original on 6 July 2015. Retrieved 6 July 2015. {{cite web}} : CS1 maint: bot: original URL status unknown (link)
19. ^ WikiLeaks [@wikileaks] (6 July 2015). "Inside malware makers "HackingTeam": hundreds of gigabytes of e-mails, files, and source code" (Tweet). Retrieved 6 July 2015 – via Twitter.
20. ^ Hacking Team on Twitter
21. ^ Ragan, Steve (5 July 2015). "HackingTeam hacked, attackers claim 400GB in dumped data". Retrieved 6 July 2015.
22. ^ Khandelwal, Swati. "Zero-Day Flash Player Exploit Disclosed In 'HackingTeam' Data Dump". Retrieved 6 July 2015.
23. ^ Pi, Peter. "Unpatched Flash Player Flaw, More POCs Found in HackingTeam Leak". Retrieved 8 July 2015.
24. ^ Adobe Systems (corporate author). "Adobe Security Bulletin". Retrieved 11 July 2015. {{cite web}} : |last= has generic name (help)
25. ^ Tang, Jack (7 July 2015). "A Look at the Open Type Font Manager Vulnerability from the HackingTeam Leak". Retrieved 8 July 2015.
26. ^ Whittaker, Zack. "HackingTeam used shockingly bad passwords". ZDNet. Retrieved 6 July 2015.
27. ^ Christian Pozzi. "unknown". Archived from the original on 7 March 2021. Retrieved 6 July 2015 – via Twitter. {{cite web}} : Cite uses generic title (help)
28. ^ Christian Pozzi. "unknown". Archived from the original on 7 March 2021. Retrieved 6 July 2015 – via Twitter. {{cite web}} : Cite uses generic title (help)
29. ^ Christian Pozzi. "unknown". Archived from the original on 23 December 2020. Retrieved 6 July 2015 – via Twitter. {{cite web}} : Cite uses generic title (help)
30. ^ "Christian Pozzi on Twitter: "Uh Oh - my twitter account was also hacked."". 6 July 2015. Archived from the original on 6 July 2015. Retrieved 6 July 2015.
31. ^ Osbourne, Charlie. "HackingTeam: We won't 'shrivel up and go away' after cyberattack". ZDNet. Retrieved 6 July 2015.
32. ^ "How HackingTeam got hacked". Ars Technica. 19 April 2016. Retrieved 15 May 2016.
33. ^ "Hacking Team's Global License Revoked by Italian Export Authorities". Privacy International. 8 April 2016. Archived from the original on 5 May 2019. Retrieved 15 May 2016.
34. ^ Kopstein, Justin (6 July 2015). "Here Are All the Sketchy Government Agencies Buying HackingTeam's Spy Tech". Vice Magazine.
35. ^ Weissman, Cale Guthrie (6 July 2015). "Hacked security company's documents show a laundry list of questionable clients". Business Insider.
36. ^ Ragan, Steve. "In Pictures: HackingTeam's hack curated". CSO Online (Australia).
37. ^ Hern, Alex (6 July 2015). "HackingTeam hacked: firm sold spying tools to repressive regimes, documents claim". The Guardian. Retrieved 22 July 2015.

38. ^ *Ragan, Steve (6 July 2015). "HackingTeam responds to data breach, issues public threats and denials". CSO Online. Retrieved 22 July 2015.*
39. ^ *Stevenson, Alastair (14 July 2015). "A whole bunch of downed government surveillance programs are about to go back online". Business Insider. Retrieved 22 July 2015.*
40. ^ *Stevenson, Alastair (8 September 2021). "Hacking Team Customer in Turkey Was Arrested for Spying on Police Colleagues [or: The Spy Story That Spun a Tangled Web]". Zetter. Retrieved 8 September 2021.*
41. ^ Jone Pierantonio. "Ecco chi ha bucato HackingTeam" Archived 6 August 2015 at the Wayback Machine. *International Business Times*. Retrieved 2 August 2015.
42. ^ Ediciones El País (8 July 2015). "HackingTeam: “Ofrecemos tecnología ofensiva para la Policía”". *El País*. Retrieved 2 August 2015.
43. ^ McGrath, Ben (25 July 2015). "*Further revelations in South Korean hacking scandal*". *World Socialist Web Site*. Retrieved 26 July 2015.
44. ^ In Cyprus (11 July 2015).Intelligence Service chief steps down Archived 2015-08-15 at the Wayback Machine. Retrieved 26 July 2015.
45. ^ Perlroth, Nicole (10 October 2012). Ahead of Spyware Conference, More Evidence of Abuse. *The New York Times* (Bits).

External links

- Official website
- HackingTeam Archives - investigative reports published by The Citizen Lab
- WikiLeaks: *The Hackingteam Archives* - searchable database of 1 million internal emails
- HackingTeam presentations in the WikiLeaks "*Spy Files*"

Hacking in the 2010s

Timeline

Major incidents

- Operation Aurora
- Australian cyberattacks
- Operation ShadowNet
- Operation Payback

2010

2011	• DigiNotar • DNSChanger • HBGary Federal • Operation AntiSec • Operation Tunisia • PlayStation • RSA SecurID compromise
2012	• LinkedIn hack • Stratfor email leak • Operation High Roller
2013	• South Korea cyberattack • Snapchat hack • Cyberterrorism Attack of June 25 • 2013 Yahoo! data breach • Singapore cyberattacks
2014	• Anthem medical data breach • Operation Tovar • 2014 celebrity nude photo leak • 2014 JPMorgan Chase data breach • Sony Pictures hack • Russian hacker password theft • 2014 Yahoo! data breach
2015	• Office of Personnel Management data breach • Hacking Team • Ashley Madison data breach • VTech data breach • Ukrainian Power Grid Cyberattack • SWIFT banking hack
2016	• Bangladesh Bank robbery • Hollywood Presbyterian Medical Center ransomware incident • Commission on Elections data breach • Democratic National Committee cyber attacks • Vietnam Airport Hacks • DCCC cyber attacks • Indian Bank data breaches • Surkov leaks • Dyn cyberattack • Russian interference in the 2016 U.S. elections • 2016 Bitfinex hack

2017	• 2017 Macron e-mail leaks • WannaCry ransomware attack • Westminster data breach • Petya cyberattack 2017 cyberattacks on Ukraine • Equifax data breach • Deloitte breach • Disqus breach
2018	• Trustico • Atlanta cyberattack • SingHealth data breach
2019	• Sri Lanka cyberattack • Baltimore ransomware attack • Bulgarian revenue agency hack • Jeff Bezos phone hacking

Hacktivism	• Anonymous associated events • CyberBerkut • GNAA • Goatse Security • Lizard Squad • LulzRaft • LulzSec • New World Hackers • NullCrew • OurMine • PayPal 14 • RedHack • TeaMp0isoN • TDO • UGNazi • Ukrainian Cyber Alliance

Advanced persistent threats	• Bureau 121 • Charming Kitten • Cozy Bear • Dark Basin • Elfin Team • Equation Group • Fancy Bear • Guccifer 2.0 • Hacking Team • Helix Kitten • Iranian Cyber Army • Lazarus Group (BlueNorOff) (AndAriel) • NSO Group • PLA Unit 61398 • PLA Unit 61486 • PLATINUM • Pranknet • Red Apollo • Rocket Kitten • Syrian Electronic Army • Tailored Access Operations • The Shadow Brokers • Yemen Cyber Army
Individuals	• George Hotz • Guccifer • Jeremy Hammond • Junaid Hussain • Kristoffer von Hassel • Mustafa Al-Bassam • MLT • Ryan Ackroyd • Sabu • Topiary • Track2 • The Jester

Major vulnerabilities publicly disclosed	• Evercookie (2010) • iSeeYou (2013) • Heartbleed (2014) • Shellshock (2014) • POODLE (2014) • Rootpipe (2014) • Row hammer (2014) • JASBUG (2015) • Stagefright (2015) • DROWN (2016) • Badlock (2016) • Dirty COW (2016) • Cloudbleed (2017) • Broadcom Wi-Fi (2017) • EternalBlue (2017) • DoublePulsar (2017) • Silent Bob is Silent (2017) • KRACK (2017) • ROCA vulnerability (2017) • BlueBorne (2017) • Meltdown (2018) • Spectre (2018) • EFAIL (2018) • Exactis (2018) • Speculative Store Bypass (2018) • Lazy FP State Restore (2018) • TLBleed (2018) • SigSpoof (2018) • Foreshadow (2018) • Microarchitectural Data Sampling (2019) • BlueKeep (2019) • Kr00k (2019)
Malware	
2010	• Bad Rabbit • SpyEye • Stuxnet
2011	• Alureon • Duqu • Kelihos • Metulji botnet • Stars

2012	• Carna • Dexter • FBI • Flame • Mahdi • Red October • Shamoon
2013	• CryptoLocker • DarkSeoul
2014	• Brambul • Carbanak • Careto • DarkHotel • Duqu 2.0 • FinFisher • Gameover ZeuS • Regin
2015	• Dridex • Hidden Tear • Rombertik • TeslaCrypt
2016	• Hitler • Jigsaw • KeRanger • MEMZ • Mirai • Pegasus • Petya (NotPetya) • X-Agent
2017	• BrickerBot • Kirk • LogicLocker • *Rensenware* ransomware • Triton • WannaCry • XafeCopy

- Grum
- Joanap
- NetTraveler
- R2D2
- Tinba
- Titanium
- Vault 7
- ZeroAccess botnet

2019

{software update}

Retrieved from "https://en.wikipedia.org/w/index.php?title=Hacking_Team&oldid=1088136701"