kbandla / APTnotes

Various public documents, whitepapers and articles about APT campaigns

391 commits 1 branch 0 releases 9 contributors

Branch: master New pull request Find file Clone or download

kbandla committed on Jun 28, 2017 Import reports till H1 2017 from aptnotes/data ... Latest commit e5034e3 on Jun 28, 2017

2008	Added PAN's report on Nitro	4 years ago
2009	Added PAN's report on Nitro	4 years ago

2010	Add another Aurora report	3 years ago
2011	Add norman's report on PaleBot from 2011	3 years ago
2012	Add PAN's report on lurid	3 years ago
2013	Add BitDefender paper on MiniDuke	3 years ago
2014	Merge pull request #103 from kbandla/deathclick	3 years ago
2015	adding minerva/clearsky copy kittens report from 2015	2 years ago
2016	Creation of 2016 folder	2 years ago
docs	Fix rtfd files	3 years ago
historical	Added PAN's report on Nitro	4 years ago
.gitignore	Added PAN's report on Nitro	4 years ago
APTnotes_summary.csv	ignore me, nothing to see here	2 years ago
README.md	Import reports till H1 2017 from aptnotes/data	a year ago
contributors.md	adding beast-fighter	2 years ago
papers.md	Merge branch 'master' of https://github.com/nyx0/APTnotes into nyx0-m…	3 years ago

README.md

APT Notes

This is a repository for various publicly-available documents and notes related to APT, sorted by year. For malware sample hashes, please see the individual reports.

gitter join chat

ARCHIVED!

> THIS REPO IS NOW MAINTAINED AT https://github.com/aptnotes/data Please update your bookmarks. This repo is backported only once in a while

- The new repo makes it easier for automation.
- To add new reports, please create a new issue.
- For more information, see the new README.

2017

- Jun 15 - North Korea Is Not Crazy
- Jun 14 - KASPERAGENT Malware Campaign resurfaces in May Election
- Jun 12 - CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations
- Jun 12 - WIN32/INDUSTROYER A new threat for industrial control systems
- Jun 07 - PLATINUM continues to evolve, find ways to maintain invisibility
- Jun 06 - Privileges and Credentials: Phished at the Request of Counsel
- May 24 - Operation Cobalt Kitty: A large-scale APT in Asia carried out by the OceanLotus Group
- May 17 - Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3
- May 14 - Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations
- May 11 - Cyber Attack Impersonating Identity Of Indian Think Tank To Target Central Bureau Of Investigation (cbi) And Possibly Indian Army Officials
- Apr 27 - APT Targets Financial Analysts with CVE-2017-0199

- Apr 07 - The Blockbuster Sequel
- Apr 03 - Lazarus Under The Hood
- Apr 03 - Operation Cloud Hopper
- Mar 28 - Dimnie: Hiding in Plain Sight
- Mar 27 - APT29 Domain Fronting With TOR
- Mar 14 - Operation Electric Powder - Who is targeting Israel Electric Company?
- Mar 07 - FIN7 Spear Phishing Campaign Targets Personnel Involved in SEC Filings
- Mar 06 - From Shamoon to StoneDrill
- Feb 27 - The Deception Project: A New Japanese-Centric Threat
- Feb 27 - The Gamaredon Group Toolset Evolution
- Feb 23 - Dissecting the APT28 Mac OS X Payload
- Feb 22 - Spear Phishing Techniques Used in Attacks Targeting the Mongolian Government
- Feb 21 - Additional Insights on Shamoon2
- Feb 20 - Lazarus' False Flag Malware
- Feb 17 - ChChes - Malware that Communicates with C&C Servers Using Cookie Headers
- Feb 16 - Breaking The Weakest Link Of The Strongest Chain
- Feb 16 - ViperRAT: The mobile APT targeting the Israeli Defense Force that should be on your radar
- Feb 15 - Operation Bugdrop: Cyberx Discovers Large-Scale Cyber-Reconnaissance Operation Targeting Ukrainian Organizations
- Feb 15 - The Full Shamoon: How the Devastating Malware Was Inserted Into Networks
- Feb 15 - Iranian PupyRAT Bites Middle Eastern Organizations
- Feb 15 - Magic Hound Campaign Attacks Saudi Targets
- Feb 12 - Lazarus & Watering-Hole Attacks
- Feb 10 - Cyber Attack Targeting Indian Navy's Submarine And Warship Manufacturer

- Feb 10 - Enhanced Analysis of GRIZZLY STEPPE Activity
- Feb 03 - KingSlayer A Supply chain attack
- Feb 03 - Several Polish banks hacked, information stolen by unknown attackers
- Feb 02 - Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society
- Jan 19 - URI Terror Attack & Kashmir Protest Themed Spear Phishing Emails Targeting Indian Embassies And Indian Ministry Of External Affairs
- Jan 15 - Bear Spotting Vol. 1: Russian Nation State Targeting of Government and Military Interests
- Jan 14 - A Pretty Dope Story About Bears: Early Indicators of Continued World Anti-Doping Agency (WADA) Targeting
- Jan 11 - At the Center of the Storm: Russia's APT28 Strategically Evolves its Cyber Operations
- Jan 05 - Foreign Cyber Threats to the United States
- Jan 05 - Mm Core In-Memory Backdoor Returns As Bigboss And Sillygoose
- Jan 05 - DragonOK Updates Toolset and Targets Multiple Geographic Regions
- Jan 05 - Iranian Threat Agent OilRig Delivers Digitally Signed Malware, Impersonates University of Oxford
- Jan 01 - The Digital Plagiarist Campaign: TelePorting the Carbanak Crew to a New Dimension

2016

- Dec 29 - GRIZZLY STEPPE - Russian Malicious Cyber Activity
- Dec 28 - Bear Hunting Season: Tracking APT28
- Dec 22 - Use of Fancy Bear Android Malware tracking of Ukrainian Artillery Units
- Dec 15 - Let It Ride: The Sofacy Group's DealersChoice Attacks Continue
- Dec 14 - PROMETHIUM and NEODYMIUM: Parallel zero-day attacks targeting individuals in Europe
- Nov 30 - Malware Actors Using Nic Cyber Security Themed Spear Phishing To Target Indian Government Organizations
- Nov 17 - It's Parliamentary: KeyBoy and the targeting of the Tibetan Community

- Nov 14 - New Carbanak / Anunak Attack Methodology
- Nov 09 - PowerDuke: Widespread Post-Election Spear Phishing Campaigns Targeting Think Tanks and NGOs
- Nov 03 - When The Lights Went Out: Ukraine Cybersecurity Threat Briefing
- Oct 27 - BLACKGEAR Espionage Campaign Evolves, Adds Japan To Target List
- Oct 27 - En Route with Sednit Part 3: A Mysterious Downloader
- Oct 26 - BITTER: A Targeted attack against Pakistan
- Oct 26 - Moonlight - Targeted attacks in the Middle East
- Oct 25 - Houdini's Magic Reappearance
- Oct 25 - En Route with Sednit Part 2: Observing the Comings and Goings
- Oct 20 - En Route with Sednit Part 1: Approaching the Target
- Oct 05 - Apt Reports And Opsec Evolution, Or: These Are Not The Apt Reports You Are Looking For
- Oct 05 - Wave your false flags! Deception tactics muddying attribution in targeted attacks
- Oct 03 - On the StrongPity Waterhole Attacks Targeting Italian and Belgian Encryption Users
- Sep 28 - Belling the BEAR
- Sep 26 - Sofacy's Komplex OS X Trojan
- Sep 18 - Hunting Libyan Scorpions
- Sep 06 - Buckeye cyberespionage group shifts gaze from US to Hong Kong
- Aug 24 - The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender
- Aug 13 - Visa Alert and Update on the Oracle Breach
- Aug 08 - Carbanak Oracle Breach
- Aug 08 - The ProjectSauron APT
- Aug 06 - Moonsoon - Analysis of an APT Campaign
- Aug 03 - Operation Manul
- Jul 08 - The Dropping Elephant - aggressive cyber-espionage in the Asian region

- Jul 07 - NetTraveler APT Targets Russian, European Interests
- Jul 07 - Unveiling Patchwork the Copy Paste APT
- Jul 01 - Espionage toolkit targeting Central and Eastern Europe uncovered
- Jul 01 - Pacifier APT
- Jun 30 - Asruex: Malware Infecting through Shortcut Files
- Jun 28 - Prince of Persia Game Over
- Jun 26 - Threat Group-4127 Targets Google Accounts
- Jun 23 - Tracking Elirks Variants in Japan: Similarities to Previous Attacks
- Jun 21 - Visiting The Bear Den A Journey in the Land of (Cyber-)Espionage
- Jun 20 - Red Line Drawn: China Recalculates Its Use Of Cyber Espionage
- Jun 20 - Findings from Analysis of DNC Intrusion Malware
- Jun 20 - Reverse-engineering DUBNIUM's Flash-targeting exploit
- Jun 17 - Flash zero-day exploit deployed by the ScarCruft APT Group
- Jun 16 - Threat Group 4127 Targets Hillary Clinton Presidential Campaign
- Jun 16 - Threat Group-4127 Targets Hillary Clinton Presidential Campaign
- Jun 14 - Group5: Syria and the Iranian Connection
- Jun 14 - New Sofacy Attacks Against US Government Agency
- Jun 09 - Reverse-engineering DUBNIUM
- Jun 09 - Operation DustySky Part 2 Indicators
- Jun 09 - Operation DustySky Part 2
- Jun 04 - Bears in the Midst: Intrusion into the Democratic National Committee
- Jun 03 - Apt Group Sends Spear Phishing Emails To Indian Government Officials
- Jun 03 - APT Group Sends Spear Phishing Emails to Indian Government Officials
- Jun 02 - IRONGATE ICS Malware: Nothing to See Here...Masking Malicious Activity on SCADA Systems

- May 29 - Stealth Falcon
- May 27 - IXESHE Derivative IHEATE Targets Users in America
- May 25 - CVE-2015-2545: overview of current threats
- May 24 - New Wekby Attacks Use DNS Requests As Command and Control Mechanism
- May 23 - Operation Ke3chang Resurfaces With New TidePool Malware
- May 23 - APT Case RUAG Technical Report
- May 23 - Targeted Attacks against Banks in the Middle East
- May 18 - Operation C-Major Actors Also Used Android BlackBerry Mobile Spyware Against Targets
- May 17 - Indian organizations targeted in Suckfly attacks
- May 17 - Operation Groundbait:Analysis of a surveillance toolkit
- May 17 - Mofang: A politically motivated information stealing adversary
- May 06 - Exploring CVE-2015-2545 and its users
- May 02 - Prince of Persia: Infy Malware Active In Decade of Targeted Attacks
- May 02 - Turbo Twist: Two 64-bit Derusbi Strains Converge
- Apr 26 - PLATINUM Targeted attacks in South and Southeast Asia
- Apr 25 - Two Bytes to $951M
- Apr 22 - The Ghost Dragon
- Apr 21 - Looking Into a Cyber-Attack Facilitator in the Netherlands (Appendix)
- Apr 21 - Looking Into a Cyber-Attack Facilitator in the Netherlands
- Apr 18 - Between Hong Kong and Burma: Tracking UP007 and SLServer Espionage Campaign
- Apr 13 - The Four Element Sword Engagement
- Mar 17 - Taiwan Presidential Election: A Case Study on Thematic Targeting
- Mar 15 - Suckfly: Revealing the secret life of your code signing certificates
- Mar 10 - Shifting Tactics Tracking Changes In Years Long Espionage Campaign Against Tibetans

- Mar 01 - Operation Transparent Tribe
- Feb 24 - FROM SEOUL TO SONY: THE HISTORY OF THE DARKSEOUL GROUP AND THE SONY INTRUSION MALWARE DESTOVER
- Feb 24 - Operation Blockbuster
- Feb 23 - Operation Duststorm
- Feb 12 - A Look Into Fysbis: Sofacy's Linux Backdoor
- Feb 09 - Poseidon Group
- Feb 08 - Know Your Enemies 2.0: A Primer on Advanced Persistent Threat Groups
- Feb 08 - Attack On French Diplomat Linked To Operation Lotus Blossom
- Feb 04 - T9000: Advanced Modular Backdoor Uses Complex Anti Analysis Techniques
- Feb 03 - Emissary Trojan Changelog: Did Operation Lotus Blossom Cause It To Evolve
- Jan 28 - BlackEnergy APT Attacks in Ukraine employ spearphishing with Word documents
- Jan 24 - Scarlet Mimic
- Jan 14 - RESEARCH SPOTLIGHT: NEEDLES IN A HAYSTACK
- Jan 11 - Uncovering the Seven Pointed Dagger
- Jan 07 - Operation Dusty Sky (indicators)
- Jan 07 - Operation Dusty Sky
- Jan 03 - BlackEnergy by the SSHBearDoor: attacks against Ukrainian news media and electric industry

2015

- Dec 23 - ELISE: Security Through Obesity
- Dec 22 - BBSRAT Attacks Targeting Russian Organizations Linked to Roaming Tiger
- Dec 16 - Dissecting the Malware Involved in the INOCNATION Campaign

- Dec 10 - Evolution of Cyber Threats in the Corporate Sector
- Dec 07 - Iran-based attackers use back door threats to spy on Middle Eastern targets
- Nov 23 - PEERING INTO GLASSRAT: A Zero Detection Trojan from China
- Nov 16 - Microsoft Security Intelligence Report (Volume 19)
- Nov 09 - Rocket Kitten: A Campaign With 9 Lives
- Oct 15 - Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation
- Oct 07 - Hacker Group Creates Network of Fake LinkedIn Profiles
- Sep 17 - THE DUKES: 7 years of Russian cyberespionage
- Sep 08 - Carbanak is packing new guns
- Aug 05 - Threat Group-3390 Targets Organizations For Cyberespionage
- Aug 04 - RSA Research Terracotta VPN: Enabler Of Advanced Threat Anonymity
- Aug 03 - Cyber war in perspective: Russian aggression against Ukraine
- Jul 31 - Operation Potao Express: Analysis Of A Cyber-Espionage Toolkit
- Jul 28 - The Black Vine Cyberespionage Group
- Jul 27 - Hammertoss: Stealthy Tactics Define A Russian Cyber Threat Group
- Jul 22 - Duke APT Group's Latest Tools: Cloud Services And Linux Support
- Jul 20 - China Hacks The Peace Palace: All Your Eez's Are Belong To Us
- Jul 20 - Watering Hole Attack On Aerospace Firm Exploits CVE-2015-5122 To Install Isspace Backdoor
- Jul 14 - Tracking Minidionis: Cozycar's New Ride Is Related To Seaduke
- Jul 13 - "Forkmeiamfamous": Seaduke, Latest Weapon In The Duke Armory
- Jul 09 - Butterfly: Corporate Spies Out For Financial Gain
- Jul 08 - Wild Neutron _ Economic Espionage Threat Actor Returns With New Tricks
- Jun 30 - Dino: The Latest Spying Malware From An Allegedly French Espionage Group Analyzed
- Jun 24 - Unfin4Ished Business

- Jun 22 - Games Are Over: Winnti Is Now Targeting Pharmaceutical Companies
- Jun 16 - Operation Lotusblossom
- Jun 15 - Target Attacks Against Tibetan And Hong Kong Groups Exploiting CVE-2014-4114
- Jun 15 - The Naikon APT: Tracking Down Geo-Political Intelligence Across APAC, One Nation At A Time
- Jun 11 - The Duqu 2.0 Technical Details
- Jun 10 - Duqu 2.0: A Comparison To Duqu
- Jun 04 - Blue Termite (Internet Watch)
- Jun 03 - An Iranian Cyber-Attack Campaign Against Targets In The Middle East
- May 29 - Oceanlotus
- May 28 - Grabit And The Rats
- May 27 - Analysis On APT-To-Be Attack That Focusing On China's Government Agency
- May 26 - Dissecting Linux/Moose: The Analysis Of A Linux Router-Based Worm Hungry For Social Networks
- May 21 - The Msnmm Campaigns: The Earliest Naikon APT Campaigns
- May 19 - Operation Oil Tanker: The Phantom Menace
- May 18 - Cmstar Downloader: Lurid And Enfal's New Cousin
- May 14 - Operation Tropic Trooper: Relying On Tried-And-Tested Flaws To Infiltrate Secret Keepers
- May 13 - Cylance Spear Team: A Threat Actor Resurfaces
- May 10 - APT28 Targets Financial Markets: Zero Day Hashes Released
- May 07 - Dissecting The Kraken
- May 05 - Targeted Attack on France's TV5Monde
- Apr 27 - Attacks Against Israeli & Palestinian Interests
- Apr 26 - Operation Clandestine Wolf _ Adobe Flash Zero-Day In APT3 Phishing Campaign
- Apr 22 - Cozyduke
- Apr 21 - The Cozyduke APT

- Apr 20 - Sofacy II_ Same Sofacy, Different Day
- Apr 18 - Operation Russiandoll: Adobe & Windows ZeroDay Exploits Likely leveraged By Russia's APT28
- Apr 15 - Hellsing Indicators Of Compromise
- Apr 15 - The Chronicles Of The Hellsing APT: The Empire Strikes Back
- Apr 12 - APT30 And The Mechanics Of A Long-Running Cyber Espionage Operation
- Apr 08 - RSA Incident Response: An APT Case Study
- Apr 07 - WINNTI Analysis
- Mar 31 - Volatile Cedar Threat Intelligence And Research
- Mar 19 - Operation Woolen-Goldfish When Kittens Go Phishing
- Mar 11 - Inside The Equationdrug Espionage Platform
- Mar 10 - Tibetan Uprising Day Malware Attacks
- Feb 27 - The Anthem Hack: All Roads Lead To China
- Feb 25 - Plugx Goes To The Registry (And India)
- Feb 25 - Southeast Asia: An Evolving Cyber Threat Landscape
- Feb 24 - Scanbox Ii
- Feb 18 - Shooting Elephants
- Feb 17 - The Desert Falcons Targeted Attacks
- Feb 16 - Carbanak APT The Great Bank Robbery
- Feb 16 - Equation Group: Questions And Answers
- Feb 16 - Operation Arid Viper: Bypassing The Iron Dome
- Feb 10 - Global Threat Intel Report
- Feb 04 - Pawn Storm Update: Ios Espionage App Found
- Feb 02 - Behind The Syrian Conflict's Digital Front Lines
- Jan 29 - Backdoor.Winnti Attackers Have A Skeleton In Their Closet?

- Jan 29 - Analysis Of A Recent Plugx Variant - P2P Plugx
- Jan 22 - An Analysis Of Regin's Hopscotch And Legspin
- Jan 22 - Scarab Attackers Took Aim At Select Russian Targets Since 2012
- Jan 22 - The Waterbug Attack Group
- Jan 20 - Reversing The Inception APT Malware
- Jan 20 - Analysis Of Project Cobra
- Jan 15 - Evolution Of Sophisticated Spyware: From Agent.Btz To Comrat
- Jan 12 - Insight In To A Strategic Web Compromise And Attack Campaign Against Hong Kong Infrastructure
- Jan 12 - Skeleton Key Malware Analysis

2014

- Dec 22 - Anunak: Apt Against Financial Institutions
- Dec 21 - Operation Poisoned Helmand
- Dec 19 - Alert (Ta14-353A) Targeted Destructive Malware
- Dec 18 - Malware Attack Targeting Syrian Isis Critics
- Dec 17 - Wiper Malware _ A Detection Deep Dive
- Dec 12 - Bots, Machines, And The Matrix
- Dec 12 - Vinself Now With Steganography
- Dec 10 - Cloud Atlas: Redoctober Apt Is Back In Style
- Dec 10 - Vulnerability, Malicious Code Appeared In The Mbr Destruction Function Using Hangul File
- Dec 10 - W32/Regin, Stage #1
- Dec 10 - W64/Regin, Stage #1
- Dec 09 - The Inception Framework: Cloud-Hosted Apt

- Dec 08 - The 'Penquin' Turla
- Dec 03 - Operation Cleaver: The Notepad Files
- Dec 01 - Hacking The Street? Fin4 Likely Playing The Market
- Nov 24 - I Am Ironman: Deep Panda Uses Sakula Malware To Target Organizations In Multiple Sectors
- Nov 24 - The Regin Platform Nation-State Ownership Of Gsm Networks
- Nov 24 - Secret Malware In European Union Attack Linked To U.S. And British Intelligence
- Nov 23 - Regin: Top-Tier Espionage Tool Enables Stealthy Surveillance
- Nov 21 - Operation Double Tap
- Nov 20 - Evil Bunny: Suspect #4
- Nov 14 - Derusbi (Server Variant) Analysis
- Nov 14 - Onionduke: Apt Attacks Via The Tor Network - F-Secure Weblog : News From The Lab
- Nov 14 - Roaming Tiger
- Nov 13 - Operation Cloudyomega: Ichitaro Zero-Day And Ongoing Cyberespionage Campaign Targeting Japan
- Nov 12 - Korplug Military Targeted Attacks: Afghanistan & Tajikistan
- Nov 11 - The Uroburos Case: New Sophisticated Rat Identified
- Nov 10 - The Darkhotel Apt A Story Of Unusual Hospitality
- Nov 10 - Darkhotel Indicators Of Compromise
- Nov 03 - Be2 Custom Plugins, Router Abuse, And Target Profiles
- Nov 03 - Operation Poisoned Handover: Unveiling Ties Between Apt Activity In Hong Kong's Pro-Democracy Movement
- Oct 31 - Operation Toohash How Targeted Attacks Work
- Oct 30 - The Rotten Tomato Campaign
- Oct 28 - Apt28: A Window Into Russia's Cyber Espionage Operations
- Oct 28 - Threat Spotlight: Group 72, Opening The Zxshell
- Oct 27 - Full Disclosure Of Havex Trojans

- Oct 27 - Micro-Targeted Malvertising Via Real-Time Ad Bidding
- Oct 27 - Scanbox Framework: Who's Affected, And Who's Using It?
- Oct 24 - Operation SMN
- Oct 24 - Leouncia And Orcarat
- Oct 23 - Modified Binaries Tor
- Oct 23 - Operation Pawn Storm Using Decoys To Evade Detection
- Oct 22 - Tactical Intelligence Bulletin Sofacy Phishing
- Oct 20 - Orcarat - A Whale Of A Tale
- Oct 14 - Threat Spotlight: Group 72
- Oct 14 - Hikit Analysis
- Oct 14 - Russian Cyber Espionage Campaign - Sandworm Team
- Oct 14 - Zoxpng Analysis
- Oct 09 - Democracy In Hong Kong Under Attack
- Oct 03 - New Indicators Of Compromise For Apt Group Nitro Uncovered
- Sep 26 - Aided Frame, Aided Direction (Because It's A Redirect)
- Sep 26 - Blackenergy & Quedagh: The Convergence Of Crimeware And Apt Attacks
- Sep 19 - Recent Watering Hole Attacks Attributed To Apt Group Th3Bug Using Poison Ivy
- Sep 18 - Cosmicduke Cosmu With A Twist Of Miniduke
- Sep 10 - Operation Quantum Entanglement
- Sep 08 - Targeted Threat Index: Characterizing And Quantifying Politically-Motivated Targeted Malware
- Sep 08 - When Governments Hack Opponents: A Look At Actors And Technology
- Sep 04 - Analysis Of Chinese Mitm On Google
- Sep 04 - Forced To Adapt: Xslcmd Backdoor Now On Os X
- Sep 03 - Darwin's Favorite Apt Group

- Aug 29 - Connecting The Dots: Syrian Malware Team Uses Blackworm For Attacks
- Aug 28 - Scanbox: A Reconnaissance Framework Used With Watering Hole Attacks
- Aug 27 - Profiling An Enigma: The Mystery Of North Korea's Cyber Threat Landscape
- Aug 27 - Nettraveler Apt Gets A Makeover For 10Th Birthday
- Aug 20 - El Machete
- Aug 07 - The Epic Turla Operation: Solving Some Of The Mysteries Of Snake/Uroboros
- Aug 06 - Operation Poisoned Hurricane
- Aug 05 - Operation Arachnophobia Caught In The Spider's Web
- Aug 04 - Sidewinder Targeted Attack Against Android In The Golden Age Of Ad Libraries
- Aug 04 - Gholee Protective Edge Themed Spear Phishing Campaign
- Aug 01 - Syrian Malware, The Ever-Evolving Threat
- Jul 31 - Energetic Bear _ Crouching Yeti
- Jul 31 - Crouching Yeti: Appendixes
- Jul 20 - Sayad (Flying Kitten) Infostealer: Is This The Work Of The Iranian Ajax Security Team?
- Jul 11 - The Eye Of The Tiger (Pitty Tiger)
- Jul 10 - Tr-25 Analysis - Turla / PNet / Snake/ Uroburos
- Jun 30 - Dragonfly: Cyberespionage Attacks Against Energy Suppliers
- Jun 20 - #9 Blitzanalysis: Embassy Of Greece Beijing - Compromise
- Jun 10 - Snake In The Grass: Python-based Malware Used For Targeted Attacks
- Jun 10 - Anatomy Of The Attack: Zombie Zero
- Jun 09 - Putter Panda
- Jun 06 - Illuminating The Etumbot Apt Backdoor
- May 21 - Rat In A Jar: A Phishing Campaign Using Unrecom
- May 20 - Miniduke Still Duking It Out

- May 13 - Cat Scratch Fever: Crowdstrike Tracks Newly Reported Iranian Actor As Flying Kitten
- May 13 - Operation Saffron Rose
- Apr 26 - New Zero-Day Exploit Targeting Internet Explorer Versions 9 Through 11 Identified In Targeted Attacks
- Mar 08 - Suspected Russian Spyware Turla Targets Europe, United States
- Mar 07 - Snake Campaign & Cyber Espionage Toolkit
- Mar 06 - The Siesta Campaign: A New Cybercrime Operation Awakens
- Feb 28 - Uroburos Highly Complex Espionage Software With Russian Roots
- Feb 25 - The French Connection: French Aerospace-Focused CVE-2014-0322 Attack Shares Similarities with 2012 Capstone Turbine Activity
- Feb 23 - Gathering In The Middle East, Operation Stteam
- Feb 20 - Mo' Shells Mo' Problems - Deep Panda Web Shells
- Feb 20 - Operation Greedywonk: Multiple Economic And Foreign Policy Sites Compromised, Serving Up Flash Zero-Day Exploit
- Feb 19 - The Monju Incident
- Feb 19 - Xtremerat: Nuisance Or Threat?
- Feb 13 - Operation Snowman: Deputydog Actor Compromises Us Veterans Of Foreign Wars Website
- Feb 11 - Unveiling Careto - The Masked Apt
- Jan 31 - Intruder File Report- Sneakernet Trojan
- Jan 21 - Emerging Threat Profile Shell_Crew
- Jan 15 - New Cdto: A Sneakernet Trojan Solution
- Jan 13 - Targeted Attacks Against The Energy Sector

2013

- Dec 31 - Energy At Risk: A Study Of It Security In The Energy And Natural Resources Industry

- Dec 20 - Etso Apt Attacks Analysis
- Dec 11 - Operation Ke3Chang Targeted Attacks Against Ministries Of Foreign Affairs
- Dec 02 - "Njrat", The Saga Continues
- Nov 11 - Supply Chain Analysis: From Quartermaster To Sunshopfireeye
- Oct 24 - Evasive Tactics: Terminator Rat
- Oct 24 - Fakem Rat: Malware Disguised As Windows Messenger And Yahoo! Messenger
- Sep 30 - World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks
- Sep 19 - 2Q Report On Targeted Attack Campaigns
- Sep 17 - Hidden Lynx: Professional Hackers For Hire
- Sep 13 - Operation Deputydog: Zero-Day (Cve-2013-3893) Attack Against Japanese Targets
- Sep 11 - The "Kimsuky" Operation: A North Korean Apt?
- Sep 10 - Operation Ephemeral Hydra: Ie Zero-Day Linked To Deputydog Uses Diskless Method
- Aug 23 - Operation Molerats
- Aug 21 - Poison Ivy: Assessing Damage And Extracting Intelligence
- Aug 19 - Byebye Shell And The Targeting Of Pakistan
- Aug 12 - Survival Of The Fittest: New York Times Attackers Evolve Quickly
- Aug 07 - The Little Malware That Could: Detecting And Defeating The China Chopper Web Shell
- Aug 02 - Where There Is Smoke, There Is Fire: South Asian Cyber Espionage Heats Up
- Aug 02 - Surtr: Malware Family Targeting The Tibetan Community
- Aug 01 - Inside Report _ Apt Attacks On Indian Cyber Space
- Aug 01 - Operation Hangover - Unveiling An Indian Cyberattack Infrastructure (Appendix)
- Jul 31 - Secrets Of The Comfoo Masters
- Jul 15 - The Plugx Malware Revisited: Introducing Smoaler
- Jul 09 - Dark Seoul Cyber Attack: Could It Be Worse?

- Jul 01 - Hunting The Shadows: In Depth Analysis Of Escalated Apt Attacks
- Jun 28 - Njrat Uncovered
- Jun 21 - A Call To Harm: New Malware Attacks Target The Syrian Opposition
- Jun 18 - Trojan.Apt.Seinup Hitting Asean
- Jun 07 - Keyboy, Targeted Attacks Against Vietnam And India
- Jun 04 - The Nettraveler (Aka Travnet)
- Jun 01 - Crude Faux: An Analysis Of Cyber Conflict Within The Oil & Gas Industries
- Jun 01 - The Chinese Malware Complexes: The Maudi Surveillance Operation
- May 30 - Analysis Of A Stage 3 Miniduke Sample
- May 20 - Operation Hangover |Executive Summary
- May 20 - Operation Hangover - Unveiling An Indian Cyberattack Infrastructure
- May 03 - Deep Panda
- Apr 17 - The Mutter Backdoor: Operation Beebus with New Targets
- Apr 13 - Winnti: More Than Just A Game
- Apr 03 - A Closer Look At Miniduke
- Apr 01 - Trojan.Apt.Banechant: In-Memory Trojan That Observes For Multiple Mouse Clicks
- Mar 28 - Analysis Of A Plugx Variant (Plugx Version 7.0)
- Mar 27 - Apt1: Technical Backstage
- Mar 20 - Dissecting Operation Troy: Cyberespionage In South Korea
- Mar 20 - The Teamspy Story - Abusing Teamviewer In Cyberespionage Campaigns
- Mar 17 - Safe A Targeted Threat
- Mar 13 - You Only Click Twice: Finfisher's Global Proliferation
- Feb 27 - Miniduke: Indicators
- Feb 27 - The Miniduke Mystery: Pdf 0-Day Government Spy Assembler 0X29A Micro Backdoor

- Feb 26 - Stuxnet 0.5: The Missing Link
- Feb 22 - Comment Crew: Indicators Of Compromise
- Feb 18 - Apt1 Exposing One Of China's Cyber Espionage Units
- Feb 12 - Targeted Cyber Attacks: Examples And Challenges Ahead
- Feb 03 - Command And Control In The Fifth Domain
- Feb 01 - Operation Beebus
- Jan 18 - Operation Red October
- Jan 14 - The Icefog Apt: A Tale Of Cloak And Three Daggers
- Jan 14 - "Red October" Diplomatic Cyber Attacks Investigation
- Jan 14 - The "Red October" Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic And Government Agencies

2012

- Nov 30 - The Many Faces Of Gh0St Rat: Plotting The Connections Between Malware Attacks
- Nov 03 - Systematic Cyber Attacks Against Israeli And Palestinian Targets Going On For A Year
- Nov 01 - Recovering From Shamoon
- Nov 01 - "Wicked Rose" And The Ncph Hacking Group
- Oct 27 - Trojan.Taidoor: Targeting Think Tanks
- Sep 07 - Iexpl0Re Rat
- Sep 06 - The Elderwood Project
- Aug 18 - The Mirage Campaign
- Aug 12 - The Voho Campaign: An In Depth Analysis
- Aug 09 - Gauss: Abnormal Distribution

- Jul 27 - The 'Madi' Infostealers - A Detailed Analysis
- Jul 25 - From Bahrain With Love: Finfisher Spy Kit Exposed?
- Jul 10 - Recent Observations In Tibet-Related Information Operations: Advanced Social Engineering For The Distribution Of Lurk Malware
- Jun 13 - Pest Control: Taming The Rats
- May 31 - Skywiper (A.K.A. Flame A.K.A. Flamer): A Complex Malware For Targeted Attacks
- May 22 - Ixeshe An Apt Campaign
- May 18 - Have I Got Newsforyou: Analysis Of Flamer C&C Server
- Apr 16 - New Version Of Osx.Sabpub & Confirmed Mac Apt Attacks
- Apr 03 - The Luckycat Hackers
- Mar 26 - Luckycat Redux: Inside An Apt Campaign With Multiple Targets In India And Japan
- Mar 13 - It'S Not The End Of The World: Darkcomet Misses By A Mile
- Mar 12 - Crouching Tiger, Hidden Dragon, Stolen Data
- Feb 29 - The Sin Digoo Affair
- Jan 03 - The Heartbeat Apt Campaign

2011

- Dec 28 - Stuxnet/Duqu: The Evolution Of Drivers
- Dec 08 - Cyber-intruder sparks response, debate
- Dec 08 - Palebot Trojan Harvests Palestinian Online Credentials
- Oct 31 - The Nitro Attacks: Stealing Secrets From The Chemical Industry
- Oct 26 - Duqu Trojan Questions And Answers
- Oct 12 - Alleged Apt Intrusion Set: 1.Php Group

- Sep 11 - Sk Hack By An Advanced Persistent Threat
- Aug 22 - The Lurid Downloader
- Aug 04 - Revealed: Operation Shady Rat
- Aug 03 - Htran And The Advanced Persistent Threat
- Aug 02 - Operation Shady Rat: Unprecedented Cyber-Espionage Campaign And Intellectual-Property Bonanza
- Jun 01 - Advanced Persistent Threats: A Decade In Review
- Apr 20 - Stuxnet Under The Microscope
- Feb 18 - Night Dragon: Specific Protection Measures For Consideration
- Feb 10 - Global Energy Cyberattacks: Night Dragon
- Feb 01 - W32.Stuxnet Dossier

2010

- Sep 03 - The Msupdater Trojan And Ongoing Targeted Attacks
- Aug 24 - Defense official discloses cyberattack
- Apr 06 - Shadows In The Cloud: Investigating Cyber Espionage 2.0
- Mar 14 - In-Depth Analysis Of Hydraq: The Face Of Cyberwar Enemies Unfolds
- Feb 24 - How Can I Tell If I Was Infected By Aurora?
- Feb 10 - Operation Aurora
- Jan 27 - Operation Aurora: Detect, Diagnose, Respond
- Jan 20 - Combating Aurora
- Jan 13 - The Command Structure Of The Aurora Botnet
- Jan 01 - Case Study: Operation Aurora

2009

- Mar 29 - Tracking Ghostnet: Investigating A Cyber Espionage Network
- Jan 18 - Impact Of Alleged Russian Cyber Attack

2008

- Nov 11 - Russian Cyberwar On Georgia
- Oct 01 - How China Will Use Cyber Warfare