# Hi-Tech Crime Trends 2016

slideshare.net/Group-IB/hitech-crime-trends-2016-73985957

Group-IB


1. 1. 2015 Q2 – 2016 Q1 HI-TECH CRIME TRENDS 2016
2. 2. Review of the Russian cybercrime market Key driver of growth – Targeted attacks Changes to previous period >>> Group-IB.COM
3. 3. TREND No.1 TARGETED ATTACKS ON BANKS AS A GLOBAL THREAT >>> Group-IB.COM
4. 4. COBALT ATMs and SWIFT TREND NO.2 GROUPS REFOCUS FROM COMPANIES TO BANKS LURK Core Banking Systems CORKOW POS terminals, ATMs, trading terminals ANUNAK Core Banking Systems, SWIFT, ATMs, payment gateways, POS terminals BUHTRAP Core Banking Systems GROUP-IB.COM/REPORTS CURRENT soon! >>> Group-IB.COM

5. 5. FORECAST TARGETED ATTACKS ON BANKS CHANGE IN FOCUS Active groups specializing in attacks on companies will threaten banks EXPANDING IN GEOGRAPHY Hackers attacking Russian banks will move their activity to other regions worldwide BROADENING COMPETENCIES Groups attacking ATMs will perform cyber thefts on SWIFT system PHISHING MAILOUTS The key vector to infect banking networks is phishing emails INVOLVING INSIDERS Hackers devote more time searching for insiders (contacts, application launch, consulting on system operation) LEGITIMATE TOOLS Criminals choose legitimate or free tools to perform attacks Arrests of Russian-speaking hacker groups have a significant impact on the global landscape of banking threats >>> Group-IB.COM
6. 6. TREND NO.3 Russian-speaking PC Trojan developers take over the world GLOBE Panda Banker (new) Shifu (new) Midas bot (Jupiter) (new) GozNym (new) Sphinx (new) Corebot (new) Atmos (new) Gozi (ISFB) Dridex Qadars Gootkit Vawtrak Tinba KINS (ZeusVM) Citadel Zeus Quakbot (Qbot) Retefe Ramnit RUSSIA Buhtrap Toplel Ranbyus RTM (new) Jupiter (new) Lurk Corkow Yebot Kronos Chtonic 16 of the 19 Trojans that have been actively used to attack companies are believed to be developed by Russian-speaking cybercriminals >>> Group-IB.COM
7. 7. FORECAST Russian-speaking PC Trojan developers take over the world CONTRACTION OF THE RUSSIAN MARKET The amount of groups, Trojans and losses from attacks will continuously decrease MOVEMENT TO NEW MARKETS New Trojans designed to attack foreign banks will be actively developed HACKERS TO SELL ACTIVE BOTNETS Some active botnets will be sold to less-experienced perpetrators WEB INJECTS Developers will add web injects to perform automated attacks FAKE WEB PAGES Fake web pages added to Trojans will enable hackers to expand the list of attacked countries SPAM MAILOUTS The key infection vector for banking Trojans >>> Group-IB.COM
8. 8. TREND NO.4 ANDROID TROJAN MARKET IS EXPANDING QUICKLY EUROPE AND USA Marcher 2.0 (new) Xbot (new) Abrvall (new) Asacub (new) Mbot 2.0 (new) T00rb00r (new) Marcher GM-bot Skunk Bilal Reich (Svpeng) RUSSIA Group 404 ApiMaps Adabot Cron1 (new) FlexNet (new) Agent.sx (new) Agent.BID (new) Honli (new) Asucub (new) FakeInst.ft (new) GM bot (new) Fake Marcher (new) Cron2 (new) Greff March Webmobil Mikorta MobiApps Xruss Tark Sizeprofit >>> Group-IB.COM
9. 9. TREND NO.4 ANDROID TROJAN MARKET EXPANDING QUICKLY NEW FRAUD SCHEMES SMS banking Transactions between cards Online banking transfers Fake mobile banking Interception of mobile banking access What causes explosive growth? >>> Group-IB.COM
10. 10. TREND NO.4 ANDROID TROJAN MARKET IS EXPANDING QUICKLY ADVANCED TROJANS Several infection stages Protecting network communications and code Fake web pages Web injects What causes explosive growth? MORE EFFECTIVE DISTRIBUTION Contextual advertising “Partner” programs Exploits >>> Group-IB.COM

11. 11. FORECAST a BOOM in banking Trojans targeting Android Thefts from companies Trojans to be adjusted to steal money from legal entities Covert infection Specialized exploit kits for Android will be released Sophisticated functionality Advanced Trojans will enable hackers to implement all attack schemes that were successfully performed on PC. Losses from attacks using Android Trojans will exceed damages from PC Trojans – THE MOST DANGEROUS THREAT to BANKS Mobile web injects Services for writing injects for mobile browsers will be offered on underground forums; Trojans will widely support web injects Increased damage Average loss will increase due to targeted attacks on companies >>> Group-IB.COM
12. 12. ON PC Active automated manipulations Passive automated manipulations All new Trojans support automated manipulations PHISHING Bypassing SMS verification using dialog windows ON ANDROID Automated transfer via SMS banking Automated transfer between cards VISHING Bypassing SMS verification using IVR TREND NO.5 COMPLETELY AUTOMATED FRAUD >>> Group-IB.COM
13. 13. FORECAST AUTOMATED FRAUD Automatic fraud on ANDROID Criminals will attack both companies and people using web injects to replace payment details. ROBOT-BASED VISHING Automated vishing attacks will be adjusted to bypass SMS verification and will become more popular AUTOMATED PHISHING The function to bypass SMS verification will make mobile Trojans the most dangerous threat to the majority of banks. With their wide distribution and automation PHISHING and ANDROID Trojans will finally replace PC Trojans. >>> Group-IB.COM
14. 14. TREND NO.6 IOT TRIGGERS THE GROWTH OF BOTNETS FOR DDOS ATTACKS MOVE AWAY AMPLIFIERS DNS, NTP, SSDP, CharGen and other types are less actively used BOTNETS REAPPEAR Criminals often use Linux servers and simple IoT devices to create botnets SOURCE CODES ARE PUBLISHED Lizard Stresser and Mirai were released publicly Dynamic IP addresses No antivirus installed 24-hours access to the Internet IoT devices are perfect bots Difficult to update and eliminate known vulnerabilities Passwords set by default 2015 450 Gbps 2016 602 Gbps 09.2016 1 Tbps >>> Group-IB.COM
15. 15. TREND NO.7 Ransomware – snowballing threat Key target – enterprises Buy access to critical data Check servers by guessing their passwords Encrypt Windows and Linux-based servers A wide variety of attacks on mobile devices and IoT >>> Group-IB.COM

16. 16. FORECAST INCREASE IN INCIDENTS WITH RANSOMWARE Wide variety of targets Mobile and IoT devices, cloud storages Average ransom will increase Newer ransomware versions will deliberately target key business assets, which will significantly raise the price of ransomware decryption keys Pinpoint attack The key target is companies with critical business processes, which cannot spend time to recover them and will pay ransoms Worms Ransomware will be distributed as cryptoworms to widely spread threats and cause significant damage Smoke Screens Encrypting ransomware will be used as a “distraction” tool in conjunction with high-profile targeted attacks, like DDoS attacks used previously An increase in attacks will stimulate the cyber risk insurance segment, which in turn will motivate criminals >>> Group-IB.COM
17. 17. TREND NO.8 Increase in attacks on critical infrastructure >>> Group-IB.COM
18. 18. THREATS AT TELECOM OPERATOR LEVEL What hackers need: Access to SS7 Hub or license for one of the following paid services: Defentek, Verint, CleverSig, Circles, Cobham Using Android Trojans TREND NO.9 NEW TOOLS FOR TARGETED ATTACKS AND ESPIONAGE What hackers obtain: Access to all the traffic Ability to decrypt SSL Access to credentials of external systems What hackers obtain: Access to geo-location Voice interception SMS interception Access to messengers, photos, and files Execution of USSD commands Password recovery Access to a cloud storage At provider level What hackers need: Access to a routing gateway or their own autonomous system (AS) What hackers obtain: Access to geo- location Voice interception SMS interception Execution of USSD commands >>> Group-IB.COM
19. 19. FORECAST ATTACKS ON CRITICAL INFRASTRUCTURE Public information Information on successful attacks will leak to journalists because of their political subtext Popularization Public reaction to successful attacks will provoke increased interest from cyber-armies and terrorists Cyber-armies Cyber-armies will attack critical infrastructure facilities Goal: espionage and control capability Terrorists Cyber-terrorists will target critical infrastructure facilities Goal: public attention, human losses ONLINE RECRUITMENT Cyber-terrorists will actively use the Internet for propagation and recruitments of technical specialists, who are able to perform targeted attacks arrests and recruitment Hackers arrested for targeted attacks on companies will be recruited by the Government >>> Group-IB.COM
20. 20. Key findings ATTACKS TOOLS Global operations Various and stealthy Automated thefts IoT, Ransomware, Spyware Authors of PC Trojans are of Russian origin TARGETS Banks Android Critical infrastructure Distribution of targeted attacks >>> Group-IB.COM
21. 21. Prevention Response Investigation Early Warning System Security Assessment DDoS Attack Prevention Anti-Piracy Brand Protection Computer Emergency Response Team CERT-GIB Forensic Services Malware Analysis and Investigation Incident Investigation Financial and Corporate Investigation Threat monitoring and analysis Threat Intelligence Detection of targeted attacks TDS TDS Polygon Early fraud detection Secure Bank Secure Portal GROUP-IB | Products & Services

22. 22. INFRASTRUCTURE Honeynet and botnet analysis Hacker community infiltration Open-source monitoring Network attack trackers TDS Sensors Behavior analysis system HUMAN INTELLIGENCE Forensics Investigations Malware monitoring and research CERT-GIB request database Security Assessment Group-IB case studies GLOBAL DATA EXCHANGE Computer incident response teams Domain registrar and hosting providers Cyber security vendors Europol, Interpol and law enforcement agencies Key regions of monitoring: Russia, the CIS and Eastern Europe, Asia Pacific, Middle East Profound human intelligence and cutting-edge technologies
23. 23. Email info@group-ib.com Phone +7 495 984-33-64 Website www.group-ib.com Facebook facebook.com/Group-IB Twitter twitter.com/GroupIB_GIB