Shadowbroker NSA Malware for everybody

Was Wann Wie Wo ist was passiert.

-diverse Meldungen über Cybercrime (DDOS Cryptolocker, CC Diebstahl
-um den 13 August ein riesigen Digitalen Vulkanausbruch oder besser ein schlechter Tag für die NSA

-Hackergruppe Shadowbroker hat die Equation-Group gehackt, Exploits und Tools werden auf einer Bitcoin Auction zum Kauf angeboten

https://blockchain.info/address/19BY2XCgbDe6WtTVbTyzM9eR3LYr6VitWK

Equation-Group -→> NSA Fronthackertruppe -eine Million Bitcoin

https://krypt3ia.wordpress.com/2016/08/19/shadowbrokers-bitcoin-transactions-now-theres-some-taint-for-you/

###

-Equation Group Cyber Weapons Auction – Invitation

How much you pay for enemies cyber weapons? Not malware you find in networks.
Both sides, RAT + LP, full state sponsor tool set?

We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic. We find Equation Group source range. We hack Equation Group. We find many many Equation Group cyber weapons. You see pictures. We give you some Equation Group files free, you see. This is good proof no? You enjoy!!! You break many things. You find many intrusions. You write many words. But not all, we are auction the best files.

Auction Instructions
- --------------------
We auction best files to highest bidder. Auction files better than stuxnet. Auction files better than free files we already give you. The party which sends most bitcoins to address: 19BY2XCgbDe6WtTVbTyzM9eR3LYr6VitWK before bidding stops is winner, we tell how to decrypt. Very important!!! When you send bitcoin you add additional output to transaction. You add OP_Return output. In Op_Return output you put your (bidder) contact info. We suggest use bitmessage or I2P-bote email address. No other information will be disclosed by us publicly. Do not believe unsigned messages. We will contact winner with decryption instructions. Winner can do with files as they please, we not release files to public.

FAQ
- ---
Q: Why I want auction files, why send bitcoin? A: If you like free files (proof), you send bitcoin. If you want know your networks hacked, you send bitcoin. If you want hack networks as like equation group, you send bitcoin. If you want reverse, write many words, make big name for self, get many customers, you send bitcoin. If want to know what we take, you send bitcoin.

Q: What is in auction files? A: Is secret. Equation Group not know what lost. We want Equation Group to bid so we keep secret. You bid against Equation Group, win and find out or bid pump price up, piss them off, everyone wins.

Q: What if bid and no win, get bitcoins back? A: Sorry lose bidding war lose bitcoin and files. Lose Lose. Bid to win! But maybe not total loss. Instead to losers we give consolation prize. If our auction raises 1,000,000 (million) btc total, then we dump more Equation Group files, same quality, unencrypted, for free, to everyone.

Q: When does auction end? A: Unknown. When we feel is time to end. Keep bidding until we announce winner.

Q: Why I trust you? A: No trust, risk. You like reward, you take risk, maybe win, maybe not, no guarantees. There could be hack, steal, jail, dead, or war tomorrow. You worry more, protect self from other bidders, trolls, and haters.

Closing Remarks
- --

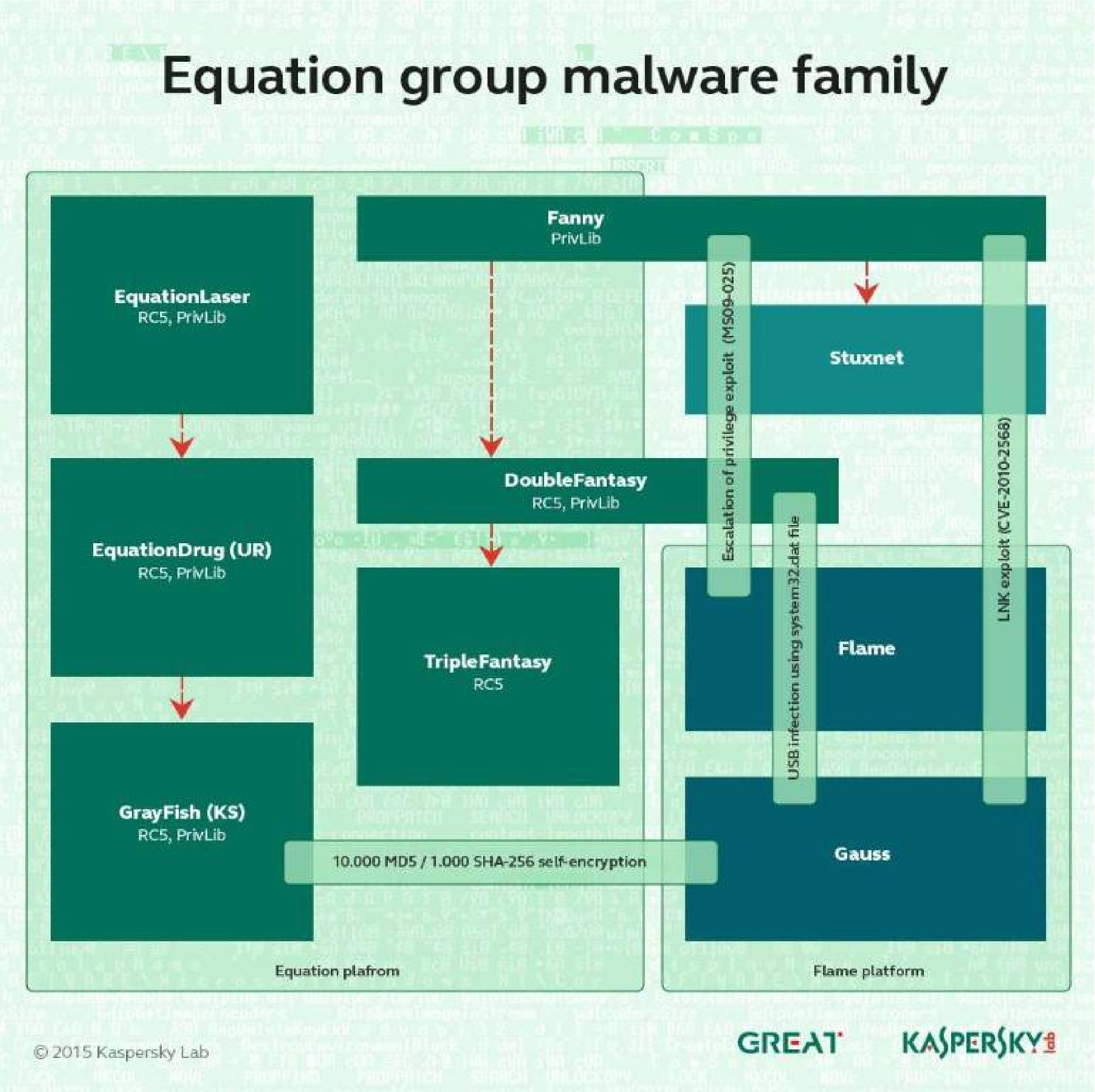
!!! Attention Wealthy Elites !!!

We have final message for "Wealthy Elites". We know what is wealthy but what is Elites? Elites is making laws protect self and friends, lie and fuck other peoples.
Elites is breaking laws, regular peoples go to jail, life ruin, family ruin, but not Elites.

Elites is breaking laws, many peoples know Elites guilty, Elites call top friends at law enforcement and government agencies, offer bribes, make promise future handjobs, (but no blowjobs).
Elites top friends announce, no law broken, no crime commit. Reporters (not call journalist) make living say write only nice things about Elites, convince dumb cattle, is just politics,
everything is awesome, check out our ads and our prostitutes.
Then Elites runs for president. Why run for president when already control country like dictatorship? What this have do with fun Cyber Weapons Auction?
We want make sure Wealthy Elite recognizes the danger cyber weapons, this message, our auction, poses to their wealth and control. Let us spell out for Elites. Your wealth and control depends on electronic data. You see what "Equation Group" can do. You see what cryptolockers and stuxnet can do. You see free files we give for free. You see attacks on banks and SWIFT in news. Maybe there is Equation Group version of cryptolocker+stuxnet for banks and financial systems? If Equation Group lose control of cyber weapons, who else lose or find cyber weapons? If electronic data go bye bye where leave Wealthy Elites? Maybe with dumb cattle? "Do you feel in charge?" Wealthy Elites, you send bitcoins, you bid in auction, maybe big advantage for you?

++

Was ist Equation-Group?
Kasperski gab diesen Namen einer Malware SoftwareFamiele nachdem sie Malware gefunden haben die Festplatten Firmware manipuliert
http://www.heise.de/security/meldung/Equation-Group-Hoechstentwickelte-Hacker-der-Welt-infizieren-u-a-Festplatten-Firmware-2550779.html]



Equation - Laser :

der Equation - Laser stammt aus dem Jahre 2004 der früheren Version und wurde weiterentwickelt zu

EQUATIONDRUG :

Eqationsdrug ist eine komplexe attackierende Plattform mit diversen Zeroday Exploits und zuladbaren Modulen mit entsprechendem Schadcode. Man kann sich das so vorstellen, wie alle Trojanerbausätze vereint. Das wurde weiterverarbeitet zu

Greyfish:

bei Greyfish kommt eine komplexe Verschlüsselung hinzu.
Ein weiterer Strang in der Equation - Group Malwaregruppe ist

FANNY:

als Computerwurm wurde es 2008 erschaffen, um Informationen
über Zielsysteme zu sammeln. Es war ausgestattet mit 2 Zeroday - Exploits.
Man kann es als Basisbausatz oder als eine angewandte Form von Stuxnet und
Flames sehen. Der nächste Enwicklungsschritt in diese Richtung ist

DOUBLE – FANTASY:

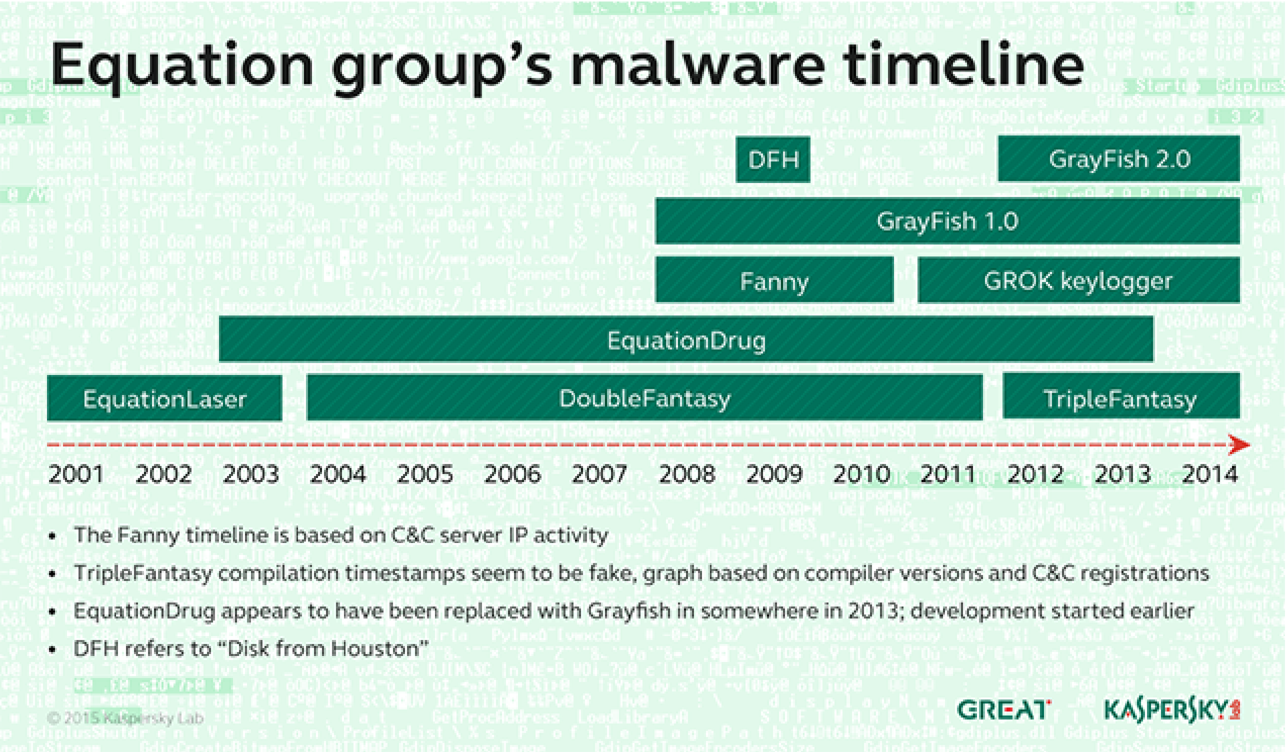
eine Art Zielobjekt – Trojaner. Wenn Double - Fantasy sein Ziel erfolgreich
gefunden und geprüft hat, werden entsprechend diverse weitere Module mit
verschiedenen Anwendungsmöglichkeiten nachgeladen und ausgeführt, wo
sich die Linie schliesst zu Equationdrug oder Greyfisch.

Wenn man jetzt diese komplexen Stukturen und ihren Aufbau zur
Totalüberwachung sieht, dann kann man nur erahnen was dahinter für eine
Entwicklungsarbeit steht.

Mehrer Tausend Entwickler Mathematiker Cryptologen
Perfektionierteste Netz an Computersabotage

Dass es sowas wie eine Equation - Group überhaupt gibt, hat Snowden mit
seinen NSA - Leaks bewiesen.
Snowden - Dokumente über Seconddate, Polarsneeze,
Turbine und Bombshell anschauen, sehen wir diverse Parallelen zu den Kaspersky – Dokumenten.

Equationgroup timeline:



Equation group's malware timeline

- The Fanny timeline is based on C&C server IP activity
- TripleFantasy compilation timestamps seem to be fake, graph based on compiler versions and C&C registrations
- EquationDrug appears to have been replaced with Grayfish in somewhere in 2013; development started earlier
- DFH refers to "Disk from Houston"

© 2015 Kaspersky Lab

weitere besondere Daten

- Stuxnet wurde 2010 gefunden

-2011 RSA secure ID gehackt

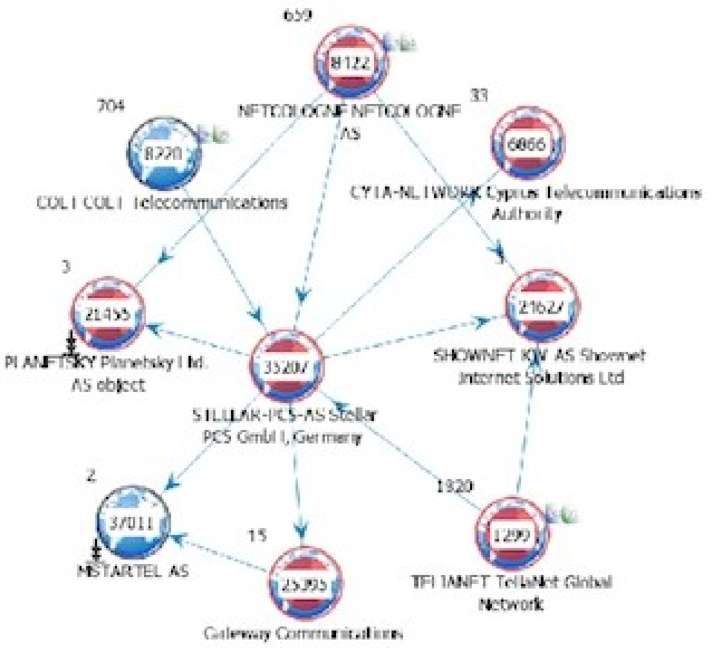
- Snowden begann im Januar 2013 mit seinen Enthüllungen.

- 2015 dokumentierte Kaspersky Lab ca. 500 Malwareinfektionen in mindestens 42 Ländern.

- grösste Malware – Sammlung,

Snoden Dokumente werden verständlicher Stella Belgacom

TOP SECRET STRAP1


659
8122
NETCOLOGNE NETCOLOGNE AS
704
8220
COLT COLT Telecommunications
33
6866
CYTA-NETWORK Cyprus Telecommunications Authority
3
21455
PLANETSKY Planetsky Ltd. AS object
35207
STELLAR-PCS-AS Stellar PCS GmbH, Germany
21627
SHOWNET KW AS Shownet Internet Solutions Ltd
2
37011
MSTARTEL AS
15
25395
Gateway Communications
1920
1299
TELIANET TeliaNet Global Network

Generated via TeasureMap

-Problem es gibt keine Gruppe oder Organisation die die Files in der Communune aufarbeitet und zb mit Stellar sprich Email Hardware vergleichen etc

Equation-Group Veröffentlichung enthält:

Exploits und tools um Hauptsächlich Firewalls zu hacken,
Übersicht:
Stand August:

Exploits

EGREGIOUSBLUNDER A remote code execution exploit for Fortigate firewalls that exploits a HTTP cookie overflow vulnerability. It affects models 60, 60M, 80C, 200A, 300A, 400A, 500A, 620B, 800, 5000, 1000A, 3600, and 3600A. The model of the firewall is detected by examining the ETag in the HTTP headers of the firewall. This is not CVE-2006-6493 as detected by Avast.

ELIGIBLEBACHELOR An exploit for TOPSEC firewalls running the TOS operation system, affecting versions 3.2.100.010, 3.3.001.050, 3.3.002.021 and 3.3.002.030. The attack vector is unknown but it has an XML-like payload that starts with `<?tos length="001e:%8.8x"?>`.

ELIGIBLEBOMBSHELL A remote code execution exploit for TOPSEC firewalls that exploits a HTTP cookie command injection vulnerability, affecting versions 3.2.100.010.1_pbc_17_iv_3 to 3.3.005.066.1. Version detection by ETag examination.

WOBBLYLLAMA A payload for the ELIGIBLEBOMBSHELL TOPSEC firewall exploit affecting version 3.3.002.030.8_003.

FLOCKFORWARD A payload for the ELIGIBLEBOMBSHELL TOPSEC firewall exploit affecting version 3.3.005.066.1.

HIDDENTEMPLE A payload for the ELIGIBLEBOMBSHELL TOPSEC firewall exploit affecting version tos_3.2.8840.1.

CONTAINMENTGRID A payload for the ELIGIBLEBOMBSHELL TOPSEC firewall exploit affecting version tos_3.3.005.066.1.

GOTHAMKNIGHT A payload for the ELIGIBLEBOMBSHELL TOPSEC firewall exploit affecting version 3.2.100.010.8_pbc_27. Has no BLATSTING support.

ELIGIBLECANDIDATE A remote code execution exploit for TOPSEC firewalls that exploits a HTTP cookie command injection vulnerability, affecting versions 3.3.005.057.1 to 3.3.010.024.1.

ELIGIBLECONTESTANT A remote code execution exploit for TOPSEC firewalls that exploits a HTTP POST paramter injection vulnerability, affecting versions 3.3.005.057.1 to 3.3.010.024.1. This exploit can be tried after ELIGIBLECANDIDATE.

EPICBANANA A privilege escalation exploit against Cisco Adaptive Security Appliance (ASA) and Cisco Private Internet eXchange (PIX) devices. Exploitation takes advantage of default Cisco credentials (password: cisco). Affects ASA versions 711, 712, 721, 722, 723, 724, 80432, 804, 805, 822, 823, 824, 825, 831, 832 and PIX versions 711, 712, 721, 722, 723, 724, 804.

ESCALATEPLOWMAN A privilege escalation exploit against WatchGuard firewalls of unknown versions that injects code via the `ifconfig` command.

EXTRABACON A remote code execution exploit against Cisco Adaptive Security Appliance (ASA) devices affecting ASA versions 802, 803, 804, 805, 821, 822, 823, 824, 825, 831, 832, 841, 842, 843, 844. It exploits an overflow vulnerability using the Simple Network Management Protocol (SNMP) and relies on knowing the target's uptime and software version.

BOOKISHMUTE An exploit against an unknown firewall using Red Hat 6.0.

FALSEMOREL Allows for the deduction of the "enable" password from data freely offered by an unspecified firewall (likely Cisco) and obtains privileged level access using only the hash of the "enable" password. Requires telnet to be installed on the firewall's inside interface.

Implants

BLATSTING A firewall software implant that is used with EGREGIOUSBLUNDER (Fortigate) and ELIGIBLEBACHELOR (TOPSEC).

BANANAGLEE A non-persistent firewall software implant for Cisco ASA and PIX devices that is installed by writing the implant directly to memory. Also mentioned in the previously leaked NSA ANT catalogue.

BANANABALLOT A BIOS module associated with an implant (likely BANANAGLEE).

BEECHPONY A firewall implant that is a predecessor of BANANAGLEE.

JETPLOW A firmware persistence implant for Cisco ASA and PIX devices that persists BANANAGLEE. Also mentioned in the previously leaked NSA ANT catalogue.

SCREAMINGPLOW Similar to JETPLOW.

BARGLEE A firewall software implant for Juniper NetScreen firewalls.

BUZZDIRECTION A firewall software implant for Fortigate firewalls.

FEEDTROUGH A technique for persisting BANANAGLEE and ZESTYLEAK implants for Juniper NetScreen firewalls. Also mentioned in the previously leaked NSA ANT catalogue.

JIFFYRAUL A module loaded into Cisco PIX firewalls with BANANAGLEE.

BANNANADAIQUIRI An implant associated with SCREAMINGPLOW. Yes, banana is spelled with three Ns this time.

POLARPAWS A firewall implant. Unknown vendor.

POLARSNEEZE A firewall implant. Unknown vendor.

ZESTYLEAK A firewall software implant for Juniper NetScreen firewalls that is also listed as a module for BANANAGLEE. Also mentioned in the previously leaked NSA ANT catalogue.

SECONDDATE A packet injection module for BANANAGLEE and BARGLEE.

BARPUNCH A module for BANANAGLEE and BARGLEE implants.

BBALL A module for BANANAGLEE implants.

BBALLOT A module for BANANAGLEE implants.

BBANJO A module for BANANAGLEE implants.

BCANDY A module for BANANAGLEE implants.

BFLEA A module for BANANAGLEE implants.

BMASSACRE A module for BANANAGLEE and BARGLEE implants.

BNSLOG A module for BANANAGLEE and BARGLEE implants.

BPATROL A module for BANANAGLEE implants.

BPICKER A module for BANANAGLEE implants.

BPIE A module for BANANAGLEE and BARGLEE implants.

BUSURPER A module for BANANAGLEE implants.

CLUCKLINE A module for BANANAGLEE implants.

Tools

BILLOCEAN Retrieves the serial number of a firewall, to be recorded in operation notes. Used in conjunction with EGREGIOUSBLUNDER for Fortigate firewalls.

FOSHO A Python library for creating HTTP exploits.

BARICE A tool that provides a shell for installing the BARGLEE implant.

DURABLENAPKIN A tool for injecting packets on LANs.

BANANALIAR A tool for connecting to an unspecified implant (likely BANANAGLEE).

PANDAROCK A tool for connecting to a POLARPAWS implant.

TURBOPANDA A tool that can be used to communicate with a HALLUXWATER implant. Also mentioned in the previously leaked NSA ANT catalogue.

TEFLONDOOR A self-destructing post-exploitation shell for executing an arbitrary file. The arbitrary file is first encrypted with a key.

1212/DEHEX Converts hexademical strings to an IP addresses and ports.

XTRACTPLEASING Extracts something from a file and produces a PCAP file as output.

NOPEN A post-exploitation shell consisting of a client and a server that encrypts data using RC6. The server is installed on the target machine.

BENIGNCERTAIN A tool that appears to be for sending certain types of Internet Key Exchange (IKE) packets to a remote host and parsing the response.

https://musalbas.com/2016/08/16/equation-group-firewall-operations-catalogue.html

https://musalbas.com/2016/08/18/equation-group-benigncertain.html

https://xorcat.net/2016/08/19/equation-group-crashing-asas-follow-up/

Technische Aspekte Praktischer Teil:

-Verzeichnisstrukrut vom Filedump

-Python Scripte (Exploit Code Shellcode)

-Vorführung Extrabacon

Was wäre nötig gewesen um solch ein Exploit selbst zu finden?
Traffic Watch zb mit transparenten firewalls

Beispiel Natalia Kasperski
Eugene Kaspersky hat sie aus Kasperski lab entlassen,
und sie gründete mit dem Programmierer
InfoWatch Traffic Monitor Enterprise

Analyse Softwore Shadowbroker

-Die software muss man halt debugen können,

ASA mit Qemu direkt laufen lassen, und Debugger einstellen

https://en.wikibooks.org/wiki/QEMU/Monitor,
beim starten der Maschine debugging dann einschalten,

Snapschot funktion und vergleichen
Syslog einstellen

Asa selber direkt debugging einschalten

https://blog.silentsignal.eu/2016/08/25/bake-your-own-extrabacon/
video anschauen
https://www.youtube.com/watch?v=KXqrovapQ5A

https://musalbas.com/2016/08/18/equation-group-benigncertain.html