Equation Group firewall operations catalogue

Published: 2016-08-16 · Archived: 2026-04-05 16:15:07 UTC

This week someone auctioning hacking tools obtained from the NSA-based hacking group "Equation Group" released a dump of around 250 megabytes of "free" files for proof alongside the auction.

The dump contains a set of exploits, implants and tools for hacking firewalls ("firewall operations"). This post aims to be a comprehensive list of all the tools contained or referenced in the dump.

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.

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.
