Avalanche (phishing group)

By Contributors to Wikimedia projects

Published: 2010-05-17 · Archived: 2026-04-02 11:11:13 UTC

From Wikipedia, the free encyclopedia

Avalanche was a criminal syndicate involved in phishing attacks, online bank fraud, and ransomware. The name also refers to the network of owned, rented, and compromised systems used to carry out that activity. Avalanche only infected computers running the Microsoft Windows operating system.

In November 2016, the Avalanche botnet was destroyed after a four-year project by an international consortium of law enforcement, commercial, academic, and private organizations.

Avalanche was discovered in December 2008, and may have been a replacement for a phishing group known as Rock Phish which stopped operating in 2008.[1] It was run from Eastern Europe and was given its name by security researchers because of the high volume of its attacks.[2][3] Avalanche launched 24% of phishing attacks in the first half of 2009; in the second half of 2009, the Anti-Phishing Working Group (APWG) recorded 84,250 attacks by Avalanche, constituting 66% of all phishing attacks. The number of total phishing attacks more than doubled, an increase which the APWG directly attributes to Avalanche.[4]

Avalanche used spam email purporting to come from trusted organisations such as financial institutions or employment websites. Victims were deceived into entering personal information on websites made to appear as though they belong to these organisations. They were sometimes tricked into installing software attached to the emails or at a website. The malware logged keystrokes, stole passwords and credit card information, and allowed unauthorised remote access to the infected computer.

Internet Identity's Phishing Trends report for the second quarter of 2009 said that Avalanche "have detailed knowledge of commercial banking platforms, particularly treasury management systems and the Automated Clearing House (ACH) system. They are also performing successful real-time man-in-the-middle attacks that defeat two-factor security tokens."[5]

Avalanche had many similarities to the previous group Rock Phish - the first phishing group which used automated techniques - but with greater in scale and volume.[6] Avalanche hosted its domains on compromised computers (a botnet). There was no single hosting provider, making difficult to take down the domain and requiring the involvement of the responsible domain registrar.

In addition, Avalanche used fast-flux DNS, causing the compromised machines to change constantly. Avalanche attacks also spread the Zeus Trojan horse enabling further criminal activity. The majority of domains which Avalanche used belonged to national domain name registrars in Europe and Asia. This differs from other phishing attacks, where the majority of domains use U.S. registrars. It appears that Avalanche chose registrars based on

their security procedures, returning repeatedly to registrars which do not detect domains being used for fraud, or which were slow to suspend abusive domains.[5][7]

Avalanche frequently registered domains with multiple registrars, while testing others to check whether their distinctive domains were being detected and blocked. They targeted a small number of financial institutions at a time, but rotated these regularly. A domain which not suspended by a registrar was re-used in later attacks. The group created a phishing "kit", which came pre-prepared for use against many victim institutions.[5][8]

Avalanche attracted significant attention from security organisations; as a result, the uptime of the domain names it used was half that of other phishing domains.[4]

In October 2009, ICANN, the organisation which manages the assignment of domain names, issued a Situation Awareness Note encouraging registrars to be proactive in dealing with Avalanche attacks.[9] The UK registry, Nominet has changed its procedures to make it easier to suspend domains, because of attacks by Avalanche.[4] Interdomain, a Spanish registrar, began requiring a confirmation code delivered by mobile phone in April 2009 which successfully forced Avalanche to stop registering fraudulent domains with them.[5]

In 2010, the APWG reported that Avalanche had been responsible for two-thirds of all phishing attacks in the second half of 2009, describing it as "one of the most sophisticated and damaging on the Internet" and "the world's most prolific phishing gang".[4]

In November 2009, security companies managed to shut down the Avalanche botnet for a short time; after this Avalanche reduced the scale of its activities and altered its *modus operandi*. By April 2010, attacks by Avalanche had decreased to just 59 from a high of more than 26,000 in October 2009, but the decrease was temporary.[1][4]

On November 30, 2016, the Avalanche botnet was destroyed at the end of a four-year project by INTERPOL, Europol, the Shadowserver Foundation,[10] Eurojust, the Luneberg (Germany) police, The German Federal Office for Information Security (BSI), the Fraunhofer FKIE, several antivirus companies organized by Symantec, ICANN, CERT, the FBI, and some of the domain registries that had been used by the group.

Symantec reverse-engineered the client malware and the consortium analyzed 130 TB of data captured during those years. This allowed it to defeat the fast-flux distributed DNS obfuscation, map the command/control structure[11] of the botnet, and identify its numerous physical servers.

37 premises were searched, 39 servers were seized, 221 rented servers were removed from the network when their unwitting owners were notified, 500,000 zombie computers were freed from remote control, 17 families of malware were deprived of c/c, and the five people who ran the botnet were arrested.

The law enforcement sinkhole server, described in 2016 as the "largest ever", with 800,000 domains served, collects the IP addresses of infected computers that request instructions from the botnet so that the ISPs owning them can inform users that their machines are infected and provide removal software.[12][13][14]

Malware deprived of infrastructure

[edit]

The following malware families were hosted on Avalanche:

- Windows-encryption Trojan horse (WVT) (a.k.a. Matsnu, Injector, Rannoh, Ransomlock.P)
- URLzone (a.k.a. Bebloh)
- Citadel
- VM-ZeuS (a.k.a. KINS)
- Bugat (a.k.a. Feodo, Geodo, Cridex, Dridex, Emotet)
- newGOZ (a.k.a. GameOverZeuS)
- Tinba (a.k.a. TinyBanker)
- Nymaim/GozNym
- Vawtrak (a.k.a. Neverquest)
- Marcher
- Pandabanker
- Ranbyus
- Smart App
- TeslaCrypt
- Trusteer App
- Xswkit

The Avalanche network also provided the c/c communications for these other botnets:

- TeslaCrypt
- Nymaim
- Corebot
- GetTiny
- Matsnu
- Rovnix
- Urlzone
- QakBot (a.k.a. Qbot, PinkSlip Bot)[15]

1. ^ Jump up to: *a b* *Greene, Tim. "Worst Phishing Pest May be Revving Up". PC World. Archived from the original on 20 May 2010. Retrieved 2010-05-17.*
2. ^ *McMillan, Robert (2010-05-12). "Report blames 'Avalanche' group for most phishing". Network World. Archived from the original on 2011-06-13. Retrieved 2010-05-17.*
3. ^ *McMillan, Robert (2010-05-12). "Report blames 'Avalanche' group for most phishing". Computerworld. Archived from the original on 16 May 2010. Retrieved 2010-05-17.*
4. ^ Jump up to: *a b c d e* *Aaron, Greg; Rod Rasmussen (2010). "Global Phishing Survey: Trends and Domain Name Use 2H2009" (PDF). APWG Industry Advisory. Retrieved 2010-05-17.*
5. ^ Jump up to: *a b c d* *"Phishing Trends Report: Analysis of Online Financial Fraud Threats Second Quarter, 2009" (PDF). Internet Identity. Retrieved 2010-05-17.* [*permanent dead link*]
6. ^ *Kaplan, Dan (2010-05-12). ""Avalanche" phishing slowing, but was all the 2009 rage". SC Magazine. Retrieved 2010-05-17.* `{{cite news}}` : CS1 maint: deprecated archival service (link)

7. ^ *Mohan, Ram (2010-05-13). "The State of Phishing - A Breakdown of The APWG Phishing Survey & Avalanche Phishing Gang". Security Week. Retrieved 2010-05-17.*
8. ^ *Naraine, Ryan. "'Avalanche' Crimeware Kit Fuels Phishing Attacks". ThreatPost. Kaspersky Lab. Archived from the original on 2010-08-02. Retrieved 2010-05-17.*
9. ^ *Ito, Yurie. "High volume criminal phishing attack known as Avalanche the delivery method for the Zeus botnet infector". ICANN Situation Awareness Note 2009-10-06. ICANN. Archived from the original on 2 April 2010. Retrieved 2010-05-17.*
10. ^ *"Shadowserver Foundation - Shadowserver - Mission".*
11. ^ *"Operation Avalanche Infograph". europol.europa.eu. Retrieved 9 November 2021.*
12. ^ *Peters, Sarah (December 1, 2016). "Avalanche Botnet Comes Tumbling Down In Largest-Ever Sinkholing Operation". darkreading.com. Retrieved December 3, 2016.*
13. ^ *Symantec Security Response (December 1, 2016). "Avalanche malware network hit with law enforcement takedown". Symantec Connect. Symantec. Retrieved December 3, 2016.*
14. ^ *Europol (December 1, 2016). "'Avalanche' network dismantled in international cyber operation". europol.europa.eu. Europol. Retrieved December 3, 2016.*
15. ^ *US-CERT (November 30, 2016). "Alert TA16-336A". us-cert.gov. CERT. Retrieved December 3, 2016.*

- Joint Cyber Operation Takes Down Avalanche Criminal Network (FBI)
