LevelBlue - Open Threat Exchange

By mohdrennis

Archived: 2026-04-02 10:50:12 UTC

TokyoX: DLL side-loading an unknown artifact (Part 2)

FileHash-MD5: 1 | **FileHash-SHA1:** 1 | **FileHash-SHA256:** 3 | **URL:** 1

A security researcher has identified and identified a threat that is being used to infect a computer and send it to the command and control server (C2) in Mexico, where the attacker is based.

- 354 Subscribers

Threat Research | FireEye Inc

Find out more about FireEye.com, the world's leading cyber security company, which provides security services to more than 1.5 million customers across the globe, and offers a wide range of products and services.

- 17 Subscribers

- 88 Subscribers

Threat Group-3390 | HttpBrowser Malware

The full list of partners has been announced by the US-based company, Secure.com, which aims to bring together more than 1,000 companies across the world to develop a range of security solutions.

- 354 Subscribers

APT group leveraging HT exploits to target a Financial Services

CVE: 1 | **Hostname:** 1

As predicted following the leak of Hacking Team exploit codes covered here, the Zscaler security research team has recently started seeing a Chinese cyber espionage group weaponizing malware payloads using the 0-day exploits found in the leaked Hacking Team archives. As such, this new attack represents a dangerous new hybrid combining the work of a notorious cyber criminal gang with Chinese cyber espionage group to attack a financial services firm. Zscaler's cloud sandboxes recently detected a Remote Access Trojan (RAT) being delivered by a well-known Chinese cyber espionage group using the Hacking Team’s 0-day exploits. This attack was specifically targeting a well-known financial services firm. The exploit files involved were identical to the Hacking Team's leaked exploit HTML, JavaScript, and ShockWave Flash 0-day files. The end payload that was installed is the HttpBrowser RAT, known to be used by the Chinese group in previous targeted attacks against governments.

- 373,184 Subscribers

Threat Group-3390 Targets Organizations for Cyberespionage

CVE: 2 | **FileHash-MD5:** 102 | **FileHash-SHA256:** 37 | **YARA:** 8 | **Domain:** 4 | **Hostname:** 61

Dell SecureWorks Counter Threat Unit(TM) (CTU) researchers investigated activities associated with Threat Group-3390[1] (TG-3390). Analysis of TG-3390's operations, targeting, and tools led CTU researchers to assess with moderate confidence the group is located in the People's Republic of China. The threat actors target a wide range of organizations: CTU researchers have observed TG-3390 actors obtaining confidential data on defense manufacturing projects, but also targeting other industry verticals and attacking organizations involved in international relations. The group extensively uses long-running strategic web compromises[2] (SWCs), and relies on whitelists to deliver payloads to select victims. In comparison to other threat groups, TG-3390 is notable for its tendency to compromise Microsoft Exchange servers using a custom backdoor and credential logger.

- 373,184 Subscribers

An analysis of exploit supply chains and digital quartermasters

CVE: 2 | **FileHash-MD5:** 81 | **URL:** 39 | **Domain:** 3 | **Hostname:** 34

On July 5, 2015 an unknown hacker publicly announced on Twitter that he had breached the internal network of Hacking Team – an Italian pentesting company known to purchase 0-day exploits and produce their own trojans. The hacker proceeded to leak archives of internal Hacking Team tools and communications. A number of tools and previously unknown exploits were discovered in the trove of data posted online. In the attached paper we will

focus on two exploits which at the time of discovery in the Hacking Team archives were unpatched. The two 0-days in question targeted Adobe Flash and were subsequently labeled CVE-2015-5119 and CVE-2015-5122.

- 373,184 Subscribers

EVASIVE MANEUVERS BY THE WEKBY GROUP

FileHash-MD5: 3 | **URL:** 2 | **Hostname:** 4

ThreatStream Labs recently became aware of a campaign beginning on 30 June 2015 by the omniprescent Wekby threat actors (a/k/a TG-0416, APT-18, Dynamite Panda). The Wekby actors have recently been observed compromising organizations in the Manufacturing, Technology and Utilities verticals, but have had a long standing interest in the HealthCare industry. This campaign uses obfuscated variants of the HTTPBrowser tool that use DNS as a control channel.

- 373,184 Subscribers

Chinese APT activity

ThreatConnect identifies Chinese targeting of two companies. Economic espionage or military intelligence?

- 474 Subscribers

Evasive Maneuvers by Wekby with Rop-packing, DNS Covert Channels

ThreatStream Labs recently became aware of a campaign beginning on 30 June 2015 by the omniprescent Wekby threat actors (a/k/a TG-0416, APT-18, Dynamite Panda). The Wekby actors have recently been observed compromising organizations in the Manufacturing, Technology and Utilities verticals, but have had a long standing interest in the HealthCare industry. This campaign uses obfuscated variants of the HTTPBrowser tool that use DNS as a control channel. This recent campaign exhibits many of the groups key characteristics to deliver a more technically advanced version of their toolkit than has previously been found. The Wekby group is keen on using phishes that purport to be from the IT helpdesk, often with links or attachments claiming to be vpn or citrix upgrades. This specific instance used a “cisco” vpnclient theme.

- 86 Subscribers

- 267 Subscribers

- 86 Subscribers

Indicators Search

Show expired indicators

We've found 97 indicators

Source: https://otx.alienvault.com/browse/pulses?q=tag:HTTPBROWSER