BIZ & IT —

Newly discovered Chinese hacking group hacked 100+ websites to use as “watering holes”

Emissary Panda group penetrated the networks of industrial espionage targets.

SEAN GALLAGHER - 8/5/2015, 9:00 PM

Chen Wu

Emissary Panda wants to eat all the industrial data—and has hacked hundreds of sites to target people with access to it.

23

LAS VEGAS—Today at the Black Hat information security conference, Dell SecureWorks researchers unveiled a report on a newly detected hacking group that has targeted companies around the world while stealing massive amounts of industrial data. The majority of the targets of the hacking group were in the automotive, electronic, aerospace, energy, and pharmaceutical industries. The group, believed to be based in China, has also targeted defense contractors, colleges and universities, law firms, and political organizations—including organizations related to Chinese minority ethnic groups.

Designated as Threat Group 3390 and nicknamed "Emissary Panda" by researchers, the hacking group has compromised victims' networks largely through "watering hole" attacks launched from over 100 compromised legitimate websites, sites picked because they were known to be frequented by those targeted in the attack.

At least 50 organizations in those industries in the US and the United Kingdom had data stolen by members of Emissary Panda. Sites targeted included the website of the Embassy of the Russian Federation in the US (as well as those of other embassies and non-governmental organizations); government agency websites around the world; manufacturing companies, many of whom were suppliers to defense contractors; and the Spanish defense manufacturer Amper. A cultural site for the Chinese Uyghur ethnic group was also used, apparently to target members of the Muslim minority for surveillance.

No zero-day vulnerabilities were used to breach targeted networks, instead "the group relied on old vulnerabilities such as CVE-2011-3544"—a near-year-old Java security hole—"and CVE-2010-0738 to compromise their targets," Dell SecureWorks' researchers reported. The group used a number of tools common to other Chinese hacking groups, but they had a few unique tools of their own with interfaces developed for Standard (Simplified) Chinese. One of these is the PlugX remote access tool, "a notorious piece of malware linked to a number of attacks and to another Threat Group, which researchers believe is also likely based out of China," according to Dell SecureWorks researchers. It also appears the group used China's Baidu search engine to perform reconnaissance on targets.

Visitors to sites exploited by Emissary Panda are directed by code embedded in the sites to a malicious webpage, which screens their IP address. If the address falls within ranges that the attackers are interested in, the malicious site waits for their next page view to drop an exploit on the desirable target's PC. (There has also been at least one victim targeted by a spear-phishing attack.) A variety of malware, including the PlugX tool, was shared with other known Chinese threat groups. But two tools used were unique to the group: ASPXTool, an Internet Information Services (IIS) specific "Web shell" used to gain access to servers inside a target's network; and the OwaAuth credential stealing tool and Web shell, used to attack Microsoft Exchange servers running the Web Outlook interface.

Once inside networks, the group generally targeted Windows network domain controllers and Exchange e-mail servers, targeting user credentials to allow them to move to other systems throughout the targeted network. They used an exploit of Internet Information Server to inject keylogger and backdoor malware onto the Exchange server. Getting into domain controller and Exchange servers gave the attackers an opportunity to steal administrator and other high-level credentials, and they could then quickly identify other points of interest and move to compromise other systems on the network—often within just two hours of the initial compromise.

READER COMMENTS 23 SHARE THIS STORY

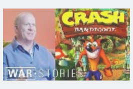
SEAN GALLAGHER
Sean was previously Ars Technica's IT and National Security Editor. A former Navy officer, systems administrator, and network systems integrator with 20 years of IT journalism experience, he lives and works in Baltimore, Maryland.

EMAIL sean.gallagher@arstechnica.com // TWITTER @thepacketrat

CHANNEL ars

How Crash Bandicoot Hacked The Original Playstation

For today’s episode of War Stories, Ars Technica sat down with Naughty Dog Co-founder Andy Gavin to talk about the hurdles in bringing the original Crash Bandicoot to gamers around the world. When Andy and his partner Jason Rubin made the decision to bring the action platforming genre into three dimensions, it required living up to their company ethos of “leaving no stone unturned” in the search for memory - even if it meant hacking Sony’s library code.



How Crash Bandicoot Hacked The Original Playstation

Myst: The challenges of CD-ROM | War Stories

Markiplier Reacts To His Top 1000 YouTube Comments

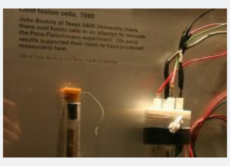
Customizing Mini 4WD Racers For High Speeds On A Small Scale

How Mind Control Saved

More videos

← PREVIOUS STORY NEXT STORY →

Related Stories


ColdFusion hack used to steal hosting provider’s customer data

Plesk control panel bug left FTC sites (and thousands more) exposed to Anons

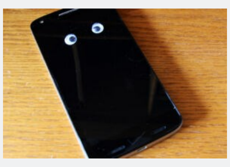
Hacked By Team System Dz
You will be held accountable Trump,
you and all your people
for every drop of blood flowing in Muslim countries
I Love Islamic state
Ohio Gov. Kasich’s website, dozens of others defaced using year-old exploit

Oracle app server hack let one attacker mine $226,000 worth of cryptocoins

Today on Ars

Don’t Panic: The comprehensive Ars Technica guide to the coronavirus [Updated 3/18]

Detroit automakers will reportedly shutter factories—but not Tesla


Android surveillanceware operators jump on the coronavirus fear bandwagon

7.5-inch e-ink display is powered completely by NFC

Steam’s new slew of 59 free demos is a perfect quarantine “game expo”

Sony details PS5’s fast SSD, variable clock rates, 3D audio tech [Updated]

Pandemic “will last 18 months or longer,” leaked US gov’t report warns

Does GameStop really need to be open during the coronavirus pandemic?

CONDÉ NAST

CNMN Collection
WIRED Media Group