

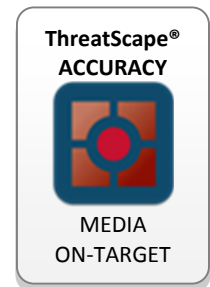
Wednesday, 2 September 2015

NATIONAL CRIME AGENCY WEBSITE OFFLINE AFTER HACKING ARRESTS

FROM THE MEDIA

Lizard Squad hackers recently attacked the UK National Crime Agency (NCA) website. The hacking group claimed responsibility for the attack via their Twitter account. The attack was allegedly in response to an operation the NCA performed in August, Vivarium, which targeted Lizard Squad members and those using the team's denial-of-service tool.

Read the Story: [Wired](#)



iSIGHT PARTNERS ANALYST COMMENT

iSIGHT Partners is highly confident that on Sept. 1, 2015, Lizard Squad conducted a successful DDoS attack against the NCA website (nationalcrimeagency.gov.uk) to protest the arrests of six UK teens accused of using the Lizard Stresser DDoS service. Lizard Squad also posted the message "New weapon coming soon," indicating that the group may be launching a new for-hire service, likely a DDoS tool, despite law enforcement efforts to interdict Lizard Squad members and customers.

RELATED iSIGHT PARTNERS REPORTS

ThreatScape Media Highlights (Police Arrest Six UK Teenagers for Using DDoS Cyber Attack Tool), 31 Aug. 2015

[15-00006466](#) (Lizard Squad Member Convicted), 13 July 2015

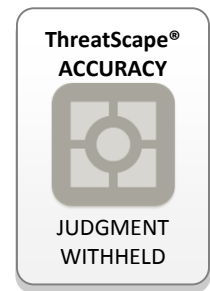
[15-00005418](#) (Group Profile: Lizard Squad), 26 June 2015

JAPANESE BANKS HIT BY NEW TROJAN, 'SHIFU'

FROM THE MEDIA

A new Trojan, dubbed "Shifu," is attacking Japanese banks and other financial institutions. The malware, discovered by IBM, may have been around since April 2015. In addition to targeting 14 Japanese banks, Shifu is also targeting electronic banking platforms used in Europe, including Austria and Germany.

Read the Story: [IT Pro Portal](#)



iSIGHT PARTNERS ANALYST COMMENT

We have not yet confirmed whether Shifu represents a new variant (bearing in mind that the malware reportedly integrates features from multiple types of existing malware) or simply a modified version of existing malware tailored to target electronic banking platforms and Japanese financial institutions. Regardless, malware operators often expand their targeting, both geographically and by victim type, after successful operations, which means successful use of this malware would likely result in the operators broadening their scope.

RELATED iSIGHT PARTNERS REPORTS

[14-29622](#) (Shiz Malware Modified to Include SAP Credential Theft), 14 Feb. 2014

[Intel-1231494](#) (New Bugat Variant 'Dridex' Represents Reemergence of Bugat with Incremental Feature Increase), 18 Sept. 2014

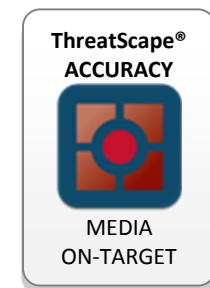
[Intel-616884](#) (Gozi Credential Theft Malware Campaign Linked to Shipping-Themed Spam), 7 Aug. 2012

YOUR NEW SMARTPHONE COULD SHIP WITH MALWARE

FROM THE MEDIA

Some third-party sellers in Asia and Europe are distributing mobile phones with pre-installed malware. G Data, a security firm, found malware on over 20 smartphone models advertised to the public as brand new. Some example brands include, Lenovo and Xiaomi. According to the research, the malware is hidden in apps the owner is most likely to use, for example, Facebook.

Read the Story: [Network World](#)



iSIGHT PARTNERS ANALYST COMMENT

Device manufacturers and resellers represent an opportunity for supply chain compromise, as devices may ship with pre-installed malware (including adware), potentially unwanted programs and programs that undermine the security practices of other software on the device. Preloading malware on to phones before selling is a time tested distribution method for malicious actors, which we have observed in China for years. Whenever possible, devices should undergo security analysis after receipt and prior to deployment into enterprise environments.

RELATED iSIGHT PARTNERS REPORTS

[15-00003244](#) (Superfish, PrivDog Demonstrate Continued Threat Third-Party Software Poses to SSL), 21 April 2015

[Intel-1220876](#) (Reprogramming Microcontroller Firmware Enables New USB Device-Based Attack Technique), 26 Aug. 2014

[Intel-355176](#) (Chinese Government Crackdown on Pre-Installed Mobile Trojans) Feb. 15, 2011

SECOND QUARTER OF 2015 SAW A RISE IN RANSOMWARE AND MOBILE MALWARE

FROM THE MEDIA

The total number of detected ransomware samples has increased 127 percent over 2014. According to Intel Security, 1.2 million new ransomware samples were identified in the second quarter of 2015. In addition to ransomware, mobile malware increased by 12 percent. The largest growth in mobile malware was found in Africa.

Read the Story: [Softpedia](#)



iSIGHT PARTNERS ANALYST COMMENT

iSIGHT Partners has observed growing underground interest in and availability of ransomware since 2014, including mobile ransomware, which corresponds to the increased detection of ransomware samples. The general increase in mobile malware is almost certainly attributable to the broadening global attack surface, including expansion to developing countries whose populace largely relies on mobile technology for business and financial transactions.

RELATED iSIGHT PARTNERS REPORTS

[15-00007688](#) ('Encryptor RaaS' Ransomware Highlights Continued Developments in Underground Economy), 26 Aug. 2015

[15-00008146](#) ('CryptoLocker' Advertised by 'MasterBass' Demonstrates Potential Developing Ransomware Threat), 17 Aug. 2015

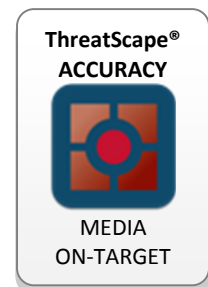
[15-00008802](#) (Notable Developments in Cyber Crime Tools During July 2015), 27 Aug. 2015

POPULAR BELKIN WI-FI ROUTERS PLAGUED BY UNPATCHED SECURITY FLAWS

FROM THE MEDIA

Several vulnerabilities have been found in the Belkin N600 DB router, a mid-range consumer wireless router. CERT indicated in an advisory that actors could conduct remote attacks to exploit the vulnerabilities, potentially directing users to malicious websites. Because the router does not require a password for accessing the management interface, actors might be able to conduct some of the attacks without authentication.

Read the Story: [IT World](#)



iSIGHT PARTNERS ANALYST COMMENT

Although these types of vulnerabilities are common, they still pose a threat to systems using consumer routers. Attacks exploiting the vulnerabilities are plausible, but exploitation of existing browser-based vulnerabilities could achieve the same result with less effort. The N600 DB router is intended for home and small office use, but certain enterprise environments may also utilize the routers for their operations. Additionally, users working from home or in small office environments could expose sensitive enterprise information if their routers are vulnerable.

RELATED iSIGHT PARTNERS REPORTS




[15-00008896](#) (Weekly Vulnerability Exploitation Report), 31 Aug. 2015

[15-00007592](#) (Hactivist Actors Utilize Routers in Retaliatory Attacks), 5 Aug. 2015

[15-00004560](#) (Routers Utilized for Reflection DDoS Attacks), 26 May 2015

About this Product

The expert analysts at iSIGHT Partners™ highlight and provide context to current media trends each day as they analyze and encapsulate the events in cyber security. Topics selected cover a broad array of cyber threats and are intended to aid readers in framing key publically discussed threats. iSIGHT Partners does not specifically endorse any third-party claims made in this material or related links, and the opinions expressed by third parties are theirs alone. The enclosed iSIGHT Partners comments and accuracy rankings are based on information available at the time of publication, and iSIGHT Partners reserves the right to hone its analytical perspectives as the threats evolve and as further intelligence is made available.

Rank	Meaning
 ThreatScape® ACCURACY MEDIA ON-TARGET	This ranking denotes a media trend in which the information reported is generally verifiable and can be correlated with our additional intelligence sources.
 ThreatScape® ACCURACY MEDIA OFF-TARGET	This ranking refers to a story in which key elements are unsubstantiated or inaccurate. A story can have a key element which is inaccurate, and the rest accurate, and still receive the ranking Off Target.
 ThreatScape® ACCURACY JUDGMENT WITHHELD	This ranking refers to a story which is complex enough that we cannot validate it in a short time, or in which the content is on the edge between on and off target.

The accuracy rating is applied through analysis of the data behind each trend based on iSIGHT Partners closed sources of information. The reason for this rating is so that our readers can quickly be alerted to trends, which are not yet substantiated or are based on information in conflict with iSIGHT Partners intelligence.

This document is developed and provided by iSIGHT Partners for direct distribution to your organization. Re-distribution or publication outside of your organization is not permitted without the expressed written permission of iSIGHT Partners. For more information on these highlights or other details on iSIGHT Partners products, please contact info@isightpartners.com or +1-214-731-4585.

If you would like to stop receiving the ThreatScape® I Media Highlights, please reply to this report and at the top of the reply state "Please unsubscribe."