DeepSight™ INTELLIGENCE

GHOST KILLER ACTOR SUPPORTING MIDDLE EAST-BASED HACKING GROUPS

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE PROFILE | SYMC - 300225 | V.1
09 JUL 2015 GMT

LEGAL NOTICE

SYMANTEC PROPRIETARY & CONFIDENTIAL - PERMITTED USE ONLY

Symantec assigns a high, medium, or low degree of confidence to assessments within its DeepSight™ Intelligence Portal Managed Adversary and Threat Intelligence (MATI) products. Confidence levels are determined against a three-point spectrum of source validity: variety and non-conflictive disparity of original sources, quality of source reporting, and reliability of source reporting. Confidence levels may be increased based on independent corroboration of information. High confidence generally suggests a solid judgment can be made, though such a judgment carries the risk of being wrong. Low confidence generally suggests tenuous inferences can be made, though information used to do so may have been questionable, fragmented, or singular.

Information Cut-Off Date: 07 Jul 2015 GMT

Ghost Killer Actor Supporting Middle East-Based Hacking Groups

DeepSight™ Intelligence | Intelligence Profile | SYMC - 300225 | V.1 | 09 Jul 2015 GMT

KEY FINDINGS

In late June 2015, the domain pocreations[.]fr was discovered hosting malware, graphics, and over 25 various defacement pages for Middle East-based hacking groups and individual hackers. As of 29 June 2015, there were more than 1 gigabyte of files located on this domain.

A Morocco-based hacker known as Ghost Killer administers the pocreations[.]fr domain. He codes malware, designs defacement pages, and hosts a variety of files for hackers on his domain.

EXECUTIVE SUMMARY

In late June 2015, DeepSight Intelligence discovered the domain pocreations[.]fr hosting files for various pro-Middle Eastern hacktivist groups and individual hackers. Ghost Killer, a Morocco-based hacker, compromised the legitimate website pocreations[.]fr in 2013 and now acts as its administrator. Ghost Killer worked for the *Office National des Chemins de Fer du Maroc* (*ONCF*) or the Moroccan National Railways in 2014. Ghost Killer has participated in hacking forums since 2010 and has coded various types of malware. Ghost Killer also designs and hosts defacement pages. He hosted a defacement page on pocreations[.]fr that was used as part of Anonymous's operations #OpCharlieHedo and #OpIsrael. The pocreations[.]fr domain held eight malware samples coded or modified by Ghost Killer including a njRAT variant. The majority of the samples were variants of Downloader.Ponik, a Trojan horse that downloads additional malware onto the victims' computer and is capable of stealing usernames and passwords from the compromised computer.

DETAILS

Ghost Killer, whose real name is Abdellah Tazroute, also goes by the moniker “tazroute.” Ghost Killer’s current Facebook page is located at facebook[.]com/tazroute and his Twitter handle is @tazroute_1. There are two additional Facebook profiles that Ghost Killer has not maintained since 2014. According to all three Facebook profiles, Ghost Killer is around 50 years old and resides in Morocco. In 2014, he was an employee for ONCF. Ghost Killer was affiliated with the hacking groups Blue Stone Hackers and Gaza Hacker as of 2010, but he stopped participating with the groups in early 2014. Ghost Killer was first seen in 2010 participating in multiple Visual Basic, Arabic-language hacking forums. His postings usually contained links to download malware such as DarkComet and Wi-Fi hacking tools. Ghost Killer participated in the 2015 Anonymous #OpIsrael activity by advertising a DDoS tool, located at http://goo[.]gl/A5iAPU, on blogs and social media accounts (see Figure 1).

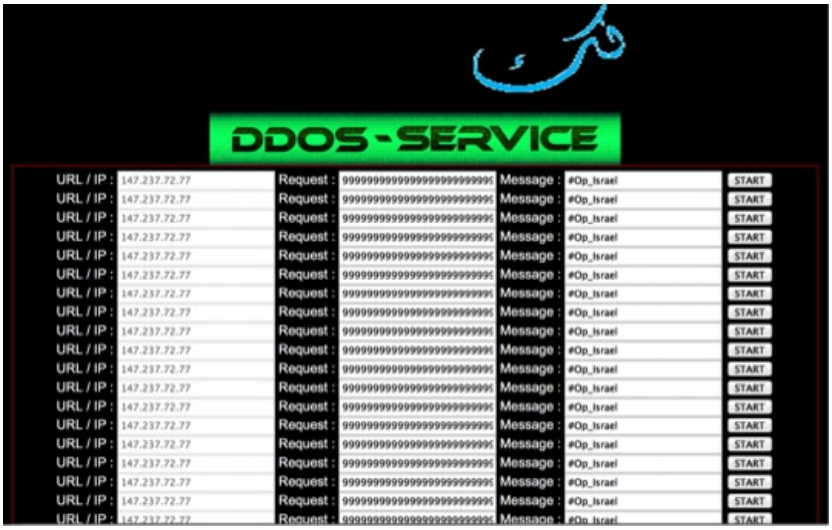

Figure 1. Screenshot of DDoS tool provided by Ghost Killer as part of #OpIsrael

Administrative Services

Ghost Killer develops malware, designs defacement pages, and hosts various files on pocreations[.]fr for Middle East-based hacking groups and individual hackers. There are over 25 defacement pages hosted on pocreations[.]fr. Several defacement pages contained on the domain are credited to Abdellah Tazroute (a.k.a. Ghost Killer). DeepSight Intelligence research in late June 2015 discovered defacement web pages for the AnonGhost and Middle East Cyber Army hacking groups on pocreations[.}fr. Defacement pages hosted by Ghost Killer include pages used by the following hacking groups or individuals: FallaG XTN, DZ mafia, DZ Force, Pirates Palestine Anonymous, Mr MAHMoud, wolf_blcak, Sniper_m@r, Anonymous DZ, Salah007, terfa DZ, mahboul DZ, Akram RoB, VirUS Algeria, AdEl, and Brinis Hacker (see Figure 2). The domain also contained several Adobe PhotoShop setup files likely used to create graphics for defacement pages.

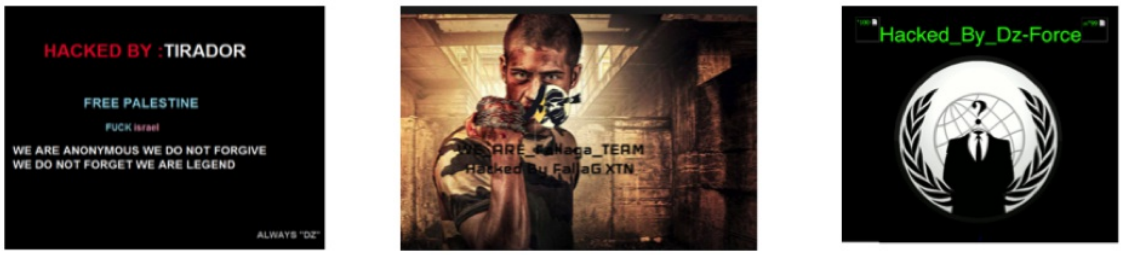

Figure 2. Sample defacement pages hosted by Ghost Killer

Malware Coding

The domain pocreations[.]fr contained eight malware files coded or modified by Ghost Killer. Some applications were written in .NET. The .NET files contain the PDB[1] string "C:\Users\ghost killer\" except for the file with the MD5 of 7f6509702278acbd545aed624d6d5d2, which contains the PDB string "c:\users\juba007\documents\visual studio 2010\." Juba007 is a pro-Muslim hacker.

The following eight malware samples with MD5 hashes were found on the domain:

File Name	MD5	Additional Information
20141107_الذ_الساعة_كية__created_by_tazroute.exe	282b6165cbc8b418614d671c3f582a1b	• Undetected by any virus vendor as of 7 July 2015. • Appears to be a Watch application. The file name includes the characters الذكية الساعة, which translates to Smart Watch.
20150104_Apple_Iphone_6.exe	570B8531C83DDB0C36B72D0F3B4234DC	• This njRAT is commonly used in the Middle East. • Drops a sample copy of windows.exe to a temporary folder and a start-up folder. A new Auto Start entry is created by adding Run keys in the registry to bypass the firewall. • The C&C is dnshostserverx.no-ip.biz on port 1177.
20150606_umt.exe	0546a5d4cc6c96f35044806a4b4af885	• Detected as Kazy. • Starts firefox.exe and connects to a defacement page hosted on pocreations[.]fr. The defacement page runs a video with the name Abdellah Tazroute displaying on the scren bottom. • Makes DNS requests to the following: o pocreations.fr (213.186.33.19) o yondarkness.googlecode.com (173.194.78.82) o upload.wikimedia.org (91.198.174.208) o www.youtube.com (173.194.40.132) o s.ytimg.com (173.194.40.129) o fonts.gstatic.com (173.194.40.152) o www.google.com (173.194.78.103)
20150606_psy.exe	be9478389d07ee3a2754591e01c251ec	• Kazy variant. • Starts firefox.exe and connects to 20150606_umt.exe, another Kazy variant.
20150606_record.exe	56A7B67F51C355E1F0AE4858B461470B	• Detected as a variant of Zbot, possibly Klovbot. • Makes a DNS request to the following: o ge.tt (54.195.252.180) o open.ge.tt (54.247.122.87)
facebook.exe	4E1791EB1DE90A47552C79235DC417E9	• Detected as Kazy. • Drops a sample copy of facebook.exe into a temporary folder and executes Firefox. It then connects to a defacement page designed by Ghost Killer on pocreations[.]fr. • Makes DNS requests to the following: o pocreations.fr (213.186.33.19) o 4.bp.blogspot.com (216.58.211.65)
15simb1a.exe	fae221dede031998aa486da60bbb1331	• Detected as a Zbot variant. • Starts firefox.exe and connects to the YouTube video at https://www.youtube.com/watch?t=107&v=4XsMAquc3wc (see Figure 3). • Makes DNS requests to the following: o www.youtube.com (173.194.45.68) o fonts.gstatic.com (173.194.45.79) o s.ytimg.com (173.194.45.69) o r3---sn-u2oxu-f5f6.googlevideo.com (188.47.194.14) o accounts.google.com (216.58.211.77) o ssl.gstatic.com (173.194.45.87) o www.youtube-nocookie.com (173.194.45.66) o apis.google.com (173.194.45.68) o i.ytimg.com (173.194.45.66) o pagead2.googlesyndication.com (173.194.45.90) o www.googletagservices.com (173.194.45.77) o www.google.com (64.233.184.105) o tpc.googlesyndication.com (173.194.45.76)
20141107_Note_Pad_tazroute.exe	95a959c2937a81a0cdd6b1af474bf358	• Undetected by anti virus vendors as of 7 July 2015.

Several of the malware samples listed in the table above are detected in Virus Total as a variant of the Kazy Trojan. Kazy variants are detected by Symantec as Downloader.Ponik, an information stealing Trojan with downloader and credential stealing capabilities.

Figure 3. YouTube video published 17 August 2012 by the user Sarah Gaga. As of 7 July 2015, the video had 23,548 views.

[1] The program database file (.PDB), which contains debugging information, is created when the file is compiled.

OUTLOOK

DeepSight Intelligence assesses Ghost Killer will continue to use the domain pocreations[.]fr to host services until the legitimate owner of the site realizes it has been compromised. In addition to Ghost Killer using the website pocreations[.]fr to host malicious files and to stage defacement files, the website has been defaced by at least three other hacking groups since 2013. DeepSight Intelligence believes Ghost Killer manages other compromised domains similar to pocreations[.]fr. By compromising legitimate websites to host malicious files, Ghost Killer's files avoid being blacklisted.

TECHNICAL DETAILS

Facebook

https://www.facebook[.]com/tazroute?_rdr=p
Inactive https://fr-fr.facebook[.]com/abdellah.tazroute

Twitter

www.twitter[.]com/tazroute_1

Hacking Websites

http://www.arabsdurra[.]com/vb/member.php?u=40325,
http://www.gazahacker[.]net/cc/member-u_14962.html

METADATA

ACTORS

Name	Facebook Account	Orkut Account	Twitter Account	Pastebin Site	Tumblr Account	Vkon takte Account
Ghost Killer	https://www.facebook[.]com/tazroute?_rdr=p		@tazroute_1			

EXTRACTED INDICATORS

Indicator	Indicator Related CVE	Indicator Type
20141107_الساعة_الذكية__created_by_tazroute.exe		file_name
282b6165cbc8b418614d671c3f582a1b		file_md5
20150104_Apple_Iphone_6.exe		file_name
570B8531C83DDB0C36B72D0F3B4234DC		file_md5
20150606_psy.exe		file_name
0546a5d4cc6c96f35044806a4b4af885		file_md5
20150606_record.exe		file_name
56A7B67F51C355E1F0AE4858B461470B		file_md5
131b4a52df4332fa7c72da603f20fca163a2963f2f6085b3a71d58549ebcc456		file_sha256
facebook.exe		file_name
4E1791EB1DE90A47552C79235DC417E9		file_md5
58e5e82d0bf6c7257bb17b228694a74a4f30da948531266ebef4b93a555418c0		file_sha256
20150606_umt.exe		file_name
be9478389d07ee3a2754591e01c251ec		file_md5
4da46c11d57b8204be6c3f5880760cd362998600a56ec8d3eba23ee59e572e72		file_sha256
15simb1a.exe		file_name

Indicator	Indicator Related CVE	Indicator Type
fae221dede031998aa486da60bbb1331		file_md5
c744f3d71768cfe3bdb4ed21486730437446e0b8bd04be7075e748e8666b25d0		file_sha256
20141107_Note_Pad_tazroute.exe		file_name
95a959c2937a81a0cdd6b1af474bf358		file_md5
c744f3d71768cfe3bdb4ed21486730437446e0b8bd04be7075e748e8666b25d0		file_sha256

FILES

Detection Name	Name	MD5	SHA 256	Malicious
	20141107_الساعة_الذكية__created_by_tazroute.exe	282b6165cbc8b418614d671c3f582a1b		Y
	20150104_Apple_Iphone_6.exe	570B8531C83DDB0C36B72D0F3B4234DC		Y
	20150606_psy.exe	0546a5d4cc6c96f35044806a4b4af885		Y
	20150606_record.exe	56A7B67F51C355E1F0AE4858B461470B	131b4a52df4332fa7c72da603f20fca163a2963f2f6085b3a71d58549ebcc456	Y
	facebook.exe	4E1791EB1DE90A47552C79235DC417E9	58e5e82d0bf6c7257bb17b228694a74a4f30da948531266ebef4b93a555418c0	Y
	20150606_umt.exe	be9478389d07ee3a2754591e01c251ec	4da46c11d57b8204be6c3f5880760cd362998600a56ec8d3eba23ee59e572e72	Y
	15simb1a.exe	fae221dede031998aa486da60bbb1331	c744f3d71768cfe3bdb4ed21486730437446e0b8bd04be7075e748e8666b25d0	Y
	20141107_Note_Pad_tazroute.exe	95a959c2937a81a0cdd6b1af474bf358	c744f3d71768cfe3bdb4ed21486730437446e0b8bd04be7075e748e8666b25d0	Y

TARGET INDUSTRIES

NAICS Code	Name
51	Information

SOURCE REGIONS

Region	Asia
Subregion	Western Asia; Southern Asia
Countries	

TARGET REGIONS

Region	Worldwide
Subregion	
Countries	

THREAT DOMAINS

Hacktivism