DeepSight™ INTELLIGENCE

MILITARY THEMES USED IN ATG13 (A.K.A. APT29) OPERATIONS TARGET NATIONAL SECURITY THINK TANKS AND US GOVERNMENT

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE REPORT | SYMC - 300250 | V.1
12 AUG 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: 08 Aug 2015 GMT

Military Themes Used in ATG13 (a.k.a. APT29) Operations Target National Security Think Tanks and US Government

DeepSight™ Intelligence | Intelligence Report | SYMC - 300250 | V.1 | 12 Aug 2015 GMT

KEY FINDINGS

Advanced Threat Group 13 (ATG13) actors sent spearphishing emails to four national security think tank organizations and one US government agency on 24 May 2015.

The malicious PDF attachment initiated an infection chain that resembled MiniDuke malware variants first reported in early 2013, but internal artifacts suggest development of this variant occurred between February and May 2015.

The crafting of the email and attachment did not display the same level of sophistication displayed in recent ATG13 operations involving the CozyDuke and Hammertoss (NetDuke) families of malware. This suggests there could be multiple teams within ATG13 that use different sets of resources.

EXECUTIVE SUMMARY

A US Department of Defense (DoD)-themed spearphishing email was used by probable Advanced Threat Group 13 (ATG13) actors to target four national security think tanks and one US government agency in late May 2015. The PDF file attachment initiates an infection chain that behaves like 2013 variants of the ATG13-linked malware family MiniDuke, including the exploitation of the same two vulnerabilities in Adobe Acrobat and Adobe Reader applications. Artifacts contained within the malware indicate that this variant was developed just prior to its deployment, between February and May 2015.

DeepSight Intelligence noted a difference in the operational sophistication between this activity and other recent ATG13 activity suggesting that multiple teams could be operating within the same threat group. This operation did not demonstrate the careful planning that is typical of an ATG13 operation and more recent malware families like CozyDuke and Hammertoss (NetDuke), which have been associated with the group's recent operations. (DeepSight Intelligence refers to this group as Advanced Threat Group 13 (ATG13).)

DETAILS

On 24 May 2015, a targeted email using the theme of a speech made by a US DoD senior official (see Figure 1) was sent to five "think tank" organizations that focus on strategic national security issues and one US government agency. Based on the profiles of the victims, this military theme was almost certainly selected to specifically appeal to the recipients at those organizations.

Figure 1. US DoD-themed email

The email's sender, John Harvey, likely refers to an individual associated with the US DoD. Based on the specific reference to the "nuclear deterrence mission," it is likely that the attackers attempted to impersonate Dr. John Harvey, the Assistant to the Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs (see Figure 2). The email address green.dinosa[@]gmail.com does not appear to be associated with Harvey and is likely attacker created.

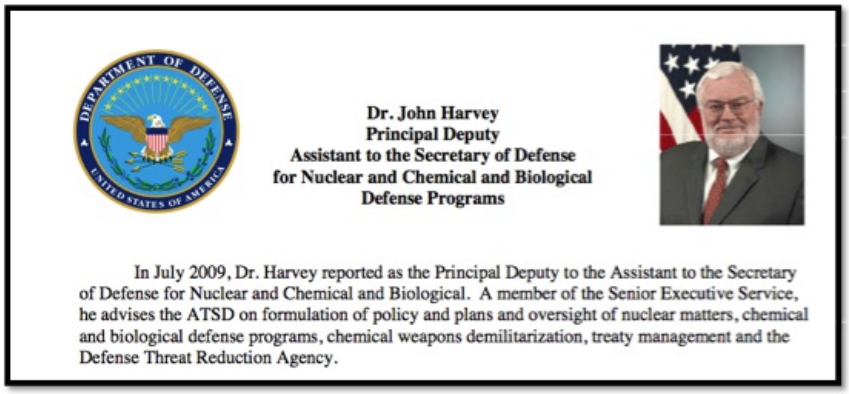
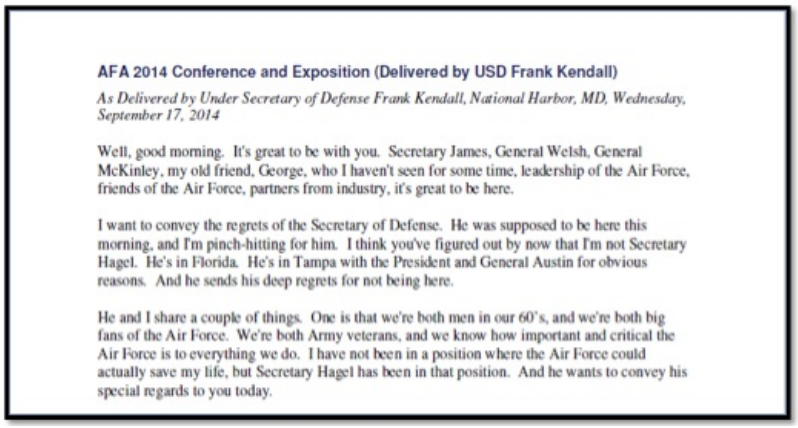


Figure 2. Profile for Dr. John Harvey who the attackers likely impersonated

The email attachment is a PDF file that poses as remarks delivered by Frank Kendall, the US DoD

Undersecretary of Defense for Acquisition, Technology, and Logistics (see Figure 3).



AFA 2014 Conference and Exposition (Delivered by USD Frank Kendall)

As Delivered by Under Secretary of Defense Frank Kendall, National Harbor, MD, Wednesday, September 17, 2014

Well, good morning. It's great to be with you. Secretary James, General Welsh, General McKinley, my old friend, George, who I haven't seen for some time, leadership of the Air Force, friends of the Air Force, partners from industry, it's great to be here.

I want to convey the regrets of the Secretary of Defense. He was supposed to be here this morning, and I'm pinch-hitting for him. I think you've figured out by now that I'm not Secretary Hagel. He's in Florida. He's in Tampa with the President and General Austin for obvious reasons. And he sends his deep regrets for not being here.

He and I share a couple of things. One is that we're both men in our 60's, and we're both big fans of the Air Force. We're both Army veterans, and we know how important and critical the Air Force is to everything we do. I have not been in a position where the Air Force could actually save my life, but Secretary Hagel has been in that position. And he wants to convey his special regards to you today.

Figure 3. Excerpt from the benign decoy PDF document (MD5: 45b19b8f2270dcfe9a2f3be3a708fba9)

The malicious file is capable of exploiting at least two vulnerabilities, CVE-2013-0640 and CVE-2013-0641, which affect several versions of Adobe Acrobat and Adobe Reader (see Figure 4). Interestingly, the body of the email contains the text "Attached is supported by Adobe version 10.X," which references versions of the platform exploited by the malicious document.

9.5.2.0	10.1.3.23
9.5.0.270	10.1.4.38
9.5.3.305	10.1.4.38ARA
10.0.1.434	10.1.5.33
10.1.0.534	11.0.0.379
10.1.2.45	11.0.1.36

Figure 4. Adobe Acrobat and Adobe Reader versions affected by CVE-2013-0640 and CVE-2013-0641

The malware communicates with the command-and-control domain reinbow5555.t25[.]us, and the URL query string includes an email address that is similar to the sender email address: dinosaurstuff324[@]gmail.com. Three likely related domains, all hosted through the free web host at t25[.]us, were also identified: reinbow.55555.t25[.]us, reinbow.555.t25[.]us, and reinbow555.t25[.]us.

Links to MiniDuke

DeepSight Intelligence assesses with high confidence that this campaign was carried out by ATG13.[1] The targeting of the national security think tanks and the US government using politically themed spearphishing is consistent with previous ATG13 campaigns. Furthermore, the malware observed in this campaign appears to be a variant of the MiniDuke malware family, which is a family that is only known to be used by ATG13. Other similarities to ATG13 include:

The use of exploits for CVE-2013-0640 and CVE-2013-0641—Adobe Acrobat and Adobe Reader

vulnerabilities first reported as associated with MiniDuke in 2013.

The JavaScript in the malicious lure PDF attachment contains Italian-language variable names consistent with previous reporting on MiniDuke.

The files “D.T” and “L2P.T” were both observed in the infection sequence of this operation. These two files have been associated with the infection sequences of previous targeting using MiniDuke as reported by Microsoft and FireEye.

Despite its similarities to MiniDuke variants discovered in early 2013, this malware sample appears to have been developed just before its deployment. Several of the dropped files have internal timestamps that range from 27 February to 24 May 2015. Additionally, a file dropped during the infection chain, MD5: 982e891b7c00be88746c05b4a67a1be7, contained the program database (PDB) file location of \ALL SPY\Mine\Backdoor\2015-NEW\Register\PDF\NewDocument\Release\Win7ElevateDll.pdb. The inclusion of “2015-NEW” in the file path indicates the possible date of development and highlights that this is likely a continuation of an existing malware family.

---

[1] ATG13 (a.k.a. APT29) has historically conducted cyber espionage operations using a number of malware families including CozyDuke, OnionDuke, MiniDuke, NetDuke and is likely based in Russia.

OUTLOOK

This operation featured a lower-than-expected attention to detail and sophistication, especially for a high-profile, nation state-aligned threat group. Characteristics of the targeted email—the use of an email address that clearly has no association with the impersonated sender’s name or role as well as minor grammatical errors in the body of the email—likely served as a red flag for recipients. Furthermore, the malicious PDF attachment relied on vulnerabilities in Adobe that were initially exploited by ATG13 as zero-day exploits in 2013, but have since been remediated by Adobe. The variation in sophistication displayed by ATG13 operations in 2015 suggests a structure that includes multiple teams with different levels of skills and resources.

TECHNICAL DETAILS

See the ***Metadata*** tab for additional technical details related to this report.

METADATA

ACTORS

Name	Facebook Account	Orkut Account	Twitter Account	Pastebin Site	Tumblr Account	Vkon takte Account
ATG13						

CAMPAIGNS

Name	ID	Status
ATG13-CE.0075	CE.0075	Active

EXTRACTED INDICATORS

Indicator	Indicator Related CVE	Indicator Type
ATG13		actor
kendall-afa 2015 conference.pdf		file_name
66f0f0bc256529aa04ecb323ea0b57f5		file_md5
fcc1978045d009c7fef9441ac57d07967b7207efcc60022f044b694a9dcf3ad7		file_sha256
D.T		file_name
9cd3649c6a8d53880e2caed01d0a6d7f		file_md5
8c3803897c70103e668c55453688852c90b2fb3ea1418dbd1cc8a2753998544a		file_sha256
L2P.T		file_name
7b3f15aa8709c6d30d03ca5cd5cca50d		file_md5
284c4433ea4d880dbf0b0aa366c5711e0ee753db837262869bc3a6b406337765		file_sha256
mag3B0.tmp		file_name
4c4e5d2b814522c41fe12ffb16b096b4		file_md5
c4547c917d8a9e027191d99239843d511328f9ec6278009d83b3b2b8349011a0		file_sha256
Regist.dll		file_name
db1d498e82c8649a01d0d824dff58aac		file_md5
0c58409ad49cd20cfcc2fda61dea2f4fcc50ff77850b839e1feff0bb5de7f8f6		file_sha256
svchost.exe		file_name
bcf879d9524932622d6df62507e2a017		file_md5
11bc1dcec99b9e3fb20ae47145120a4da7ef462a0366685fd0ddea8392a43ece		file_sha256
980fd6c38f8c20e94ef0f3adf649780c		file_md5
982e891b7c00be88746c05b4a67a1be7		file_md5
phpsend.dll		file_name

Indicator	Indicator Related CVE	Indicator Type
94E0AF1D3A0DA4630D44AADEA42D6960		file_md5
1085049ab4c5cb05165b82a7c47da79a8c1d59ce409f20fbcf3beb9285a43cd8		file_sha256
4475edf4ef1bc64ffe334078b4b4713f		file_md5
8974e88a950ff99691714924b391ba64cde1500c8ff914241e12c62f6c7080c6		file_sha256
Regist64.dll		file_name
35cc93f5d4bfee69974740cbed67b4d6		file_md5
9c17f68b1d932d16aa83c2ce121c91e52be9686104678d42da2c7a0a4e42f499		file_sha256
undefined		file_name
66f0f0bc256529aa04ecb323ea0b57f5		file_md5
fcc1978045d009c7fef9441ac57d07967b7207efcc60022f044b694a9dcf3ad7		file_sha256
reinbow5555.t25.us		domain
reinbow.55555.t25.us		domain
reinbow555.t25.us		domain
reinbow.555.t25.us		domain
www.reinbow5555.t25.us/mainmenu.php		url
green.dinosa@gmail.com		email_from_address
dinosaurstuff324@gmail.com		email_from_address

FILES

Detection Name	Name	MD5	SHA 256	Malicious
Trojan.Pidief	kendall-afa 2015 conference.pdf	66f0f0bc256529aa04ecb323ea0b57f5	fcc1978045d009c7fef9441ac57d07967b7207efcc60022f044b694a9dcf3ad7	y
	D.T	9cd3649c6a8d53880e2caed01d0a6d7f	8c3803897c70103e668c55453688852c90b2fb3ea1418dbd1cc8a2753998544a	y
	L2P.T	7b3f15aa8709c6d30d03ca5cd5cca50d	284c4433ea4d880dbf0b0aa366c5711e0ee753db837262869bc3a6b406337765	y
	mag3B0.tmp	4c4e5d2b814522c41fe12ffb16b096b4	c4547c917d8a9e027191d99239843d511328f9ec6278009d83b3b2b8349011a0	y
	Regist.dll	db1d498e82c8649a01d0d824dff58aac	0c58409ad49cd20cfcc2fda61dea2f4fcc50ff77850b839e1feff0bb5de7f8f6	y
	svchost.exe	bcf879d9524932622d6df62507e2a017	11bc1dcec99b9e3fb20ae47145120a4da7ef462a0366685fd0ddea8392a43ece	y
		980fd6c38f8c20e94ef0f3adf649780c		y
		982e891b7c00be88746c05b4a67a1be7		y
	phpsend.dll	94E0AF1D3A0DA4630D44AADEA42D6960	1085049ab4c5cb05165b82a7c47da79a8c1d59ce409f20fbcf3beb9285a43cd8	y
		4475edf4ef1bc64ffe334078b4b4713f	8974e88a950ff99691714924b391ba64cde1500c8ff914241e12c62f6c7080c6	y

Detection Name	Name	MD5	SHA 256	Malicious
	Regist64.dll	35cc93f5d4bfee69974740cbed67b4d6	9c17f68b1d932d16aa83c2ce121c91e52be9686104678d42da2c7a0a4e42f499	y
	Kendall-AFA 2014 Conference-17Sept14.pdf	45b19b8f2270dcfe9a2f3be3a708fba9		n
Trojan.Pidief	kendall-afa 2015 conference.pdf	66f0f0bc256529aa04ecb323ea0b57f5	fcc1978045d009c7fef9441ac57d07967b7207efcc60022f044b694a9dcf3ad7	y

TARGET INDUSTRIES

NAICS Code	Name
92	Public Administration
8133	Social Advocacy Organizations

SOURCE REGIONS

Region	Europe
Subregion	Eastern Europe
Countries	Russian Federation

TARGET REGIONS

Region	Americas
Subregion	North America
Countries	United States

THREAT DOMAINS

Cyber Espionage