GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

www.fidelissecurity.com
www.threatgeek.com
@FidSecSys
+1800.652.4020

Fidelis Threat Advisory #1010

"njRAT", The Saga Continues

December 2, 2013

Document Status: FINAL
Last Revised: 2013-12-02

Executive Summary

In June 2013, we released a paper containing information about the njRAT malware that included its functionality, indicators of compromise, and campaign codes used on the variants we had identified. (http://www.fidelissecurity.com/threatadvisory).

To this day, we continue to observe waves of blunt phishing attacks from compromised hosts in the Middle East, showing threat actors using multiple tools (including njRAT, AdwindRAT, Xtreme RAT, and H-Worm) in clustered phishing attacks against the same targets. Some of these attacks continue to target the U.S. telecommunications sector with threat actors sending phishing emails using business-oriented lures containing the aforementioned tools or links to websites that serve these tools.

Additionally, we continue to directly observe significant activity from threat actors sending commands to the victim systems in the Middle East.

Further, we are observing attackers using the following obfuscators to make detection of this malware specimen more difficult for security analysts:

- .NetShrink (http://www.pelock.com/products/netshrink)
- Confuser v1.9.0.0 (http://confuser.codeplex.com/)
- .NET Reactor (http://www.eziriz.com/)

This document provides details of the njRAT campaign codes used, versions, ports, and CnC nodes currently observed sending commands to victim systems. It's also clear that threat actors are actively using the following version of njRAT: 0.3.6, 0.4.1a, 0.5.0E, 0.6.4.

Threat Overview

"njRAT" is a robust remote access trojan (RAT) which upon reaching and infecting an end-point, allows the attacker to have full control over the victim system. Among other things, with this access, the attacker could start scanning other systems in the victim network to perform lateral movement.

Indicators and Mitigation Strategies

The following table contains information about the observed CnC nodes, ports, campaign codes, and njRAT versions:

CnC	Port	CnC GeoLocation	Campaign Code (Base64 encoded)	Campaign Code (Base64 decoded)	Version
105.129.18.216	1177	Morocco	SGFja2VkIEJ5IEPDoHBpaVRvc184NEFERTAyRA==	Hacked By CÃ piiTos_84ADE02D	0.6.4
105.157.2.178	1177	Morocco	S3J5c3RhbF84NEFERTAyRA==	Krystal_84ADE02D	0.5.0E
108.62.213.238	1177	Phoenix, AZ, United States	QkJNIFBJTl8xQ0NDRjY5Ng==	BBM PIN_1CCCF696	0.6.4
108.62.213.67	1177	Phoenix, AZ, United States	QkJNIFBJTl8xQ0NDRjY5Ng==	BBM PIN_1CCCF696	0.6.4
122.151.223.203	1177	Melbourne, Australia	am5vbjlfQTY3QzdDMDE=	jnon9_A67C7C01	0.6.4
145.255.78.228	1177	Muscat, Oman	WHhYX1h4WF8yMEJGMDgzQg==	XxX_XxX_20BF083B	0.5.0E
149.200.131.81	1177	Jordan	SGFjS2VkX0RFNkEyMENB	HacKed_DE6A20CA	0.6.4
149.200.224.196	1177	Jordan	SGFjS2VkX0RFNkEyMENB	HacKed_DE6A20CA	0.6.4
159.0.83.175	100	Khobar, Saudi Arabia	SGFjS2VkXzI0NjlFQTI5	HacKed_2469EA29	0.5.0E
178.238.189.53	1177	Amman, Jordan	QkJNIFBJTl8xQ0NDRjY5Ng==	BBM PIN_1CCCF696	0.6.4
188.121.234.17	1177	Paris, France	SGFjS2VkX0I0MkY4NjAz	HacKed_B42F8603	0.6.4
188.121.236.87	1177	Paris, France	SGFjS2VkX0I0MkY4NjAz	HacKed_B42F8603	0.6.4
188.121.242.49	1177	Paris, France	SGFjS2VkX0I0MkY4NjAz	HacKed_B42F8603	0.6.4
188.50.60.154	1177	Jiddah, Saudi Arabia	d2luMzJfMzRDOEM5QkY=	win32_34C8C9BF	0.6.4
188.51.30.43	1177	Jiddah, Saudi Arabia	SGFjS2VkXzRDMTBDRTND	HacKed_4C10CE3C	0.6.4
188.51.69.179	1177	Jiddah, Saudi Arabia	SGFjS2VkXzc2MTQ4QjVG	HacKed_76148B5F	0.5.0E
188.53.13.164	1177	Riyadh, Saudi	TXIuRk9YX0VGRTE3Q	Mr.FOX_EFE17AA	0.4.1a

		Arabia	UE=		
188.55.10.93	1177	Jiddah, Saudi Arabia	SGFjS2VkX0YyNjE4MThG	HacKed_F261818F	0.5.0E
188.66.233.10	192	Muscat, Oman	SC1Xb3JtXzU4MzMzMTFD	H-Worm_5833311C	0.5.0E
197.1.104.120	1177	Tunisia	YnkgYW5nbGUxMF8yNDMzM0Q2Qg==	by angle10_24333D6B	0.6.4
197.200.4.207	1177	Algeria	SGFjS2VkXzVFNjM3QTM0	HacKed_5E637A34	0.6.4
197.205.71.16	1177	Algeria	SGFjS2VkXzVFNjM3QTM0	HacKed_5E637A34	0.6.4
197.205.81.38	1177	Algeria	SGFjS2VkXzVFNjM3QTM0	HacKed_5E637A34	0.6.4
197.39.177.138	1177	Egypt	4paRIE5lVyBVc2VS4paRIF83RTFFQUFCNw==	NeW UseR _7E1EAAB7	0.4.1a
197.39.229.96	1177	Egypt	4paRIE5lVyBVc2VS4paRIF9GRTQwOEVFRQ==	NeW UseR _FE408EEE	0.4.1a
37.106.93.153	1177	Riyadh, Saudi Arabia	2KfZhNi52YrYryDYudmA2YDZitiv2YrZhiDZhdi52KfZg9mFX0Y4REJDOUMz	العيد عـيدين معاكم_F8DBC9C3	0.4.1a
37.16.55.155	1177	Saudi Arabia	2LHZiNin2KrYsV9DNkU4NTI4NA==	رواتر_C6E85284	0.5.0E
37.200.239.243	1177	Oman	VFRUVF81MEMwNDYwNA==	TTTT_50C04604	0.5.0E
37.238.194.107	1177	Iraq	2YLZhtin2LUg2KjYutiv2KfYr18yNDMzM0Q2Qg==	(0xD982D986D8A7D8B520D8A8D8BAD8AFD8A7D8AF)_24333D6B Potential HEX-2-String: قناص بغداد Potential translation to English: "Baghdad Sniper"	0.6.4
37.238.233.102	1177	Iraq	SGFjS2VkX0I4MTkzOTEy	HacKed_B8193912	0.5.0E
41.103.74.108	1177	Ouled Yaïch, Algeria	dmljdGltXzI0MzMzRDZC	victim_24333D6B	0.6.4

41.104.68.83	1177	Algeria	dmljdGltXzI0MzMzRDZC	victim_24333D6B	0.6.4
41.107.233.206	1177	Algeria	MjAxM18xRUYwNzBENA==	2013_1EF070D4	0.4.1a
41.230.233.96	1177	Safaqis, Tunisia	SGFjS2VkXzRBQjAwNEQ4	HacKed_4AB004D8	0.5.0E
41.237.75.126	1177	Cairo, Egypt	2YfZh9mH2YcgXzI0MzMzRDZC	(0xD987D987D987D98720)_24333D6B Potential HEX-2-String: هههه Potential translation to English: "Haha"	0.6.4
41.251.165.158	1177	Casablanca, Morocco	REE3aWFfNjBEMDUwQzM=	DA7ia_60D050C3	0.5.0E
41.252.201.131	1177	Libya	4pyrLS3il48g4pyYSM6sY2tlxqbinJgg4pePLS3inKtfNDQ1RUJDMjc=	☆--● ✘HáckeR✘ ●--☆_445EBC27	0.6.4
41.252.227.78	1177	Benghazi, Libya	4pyrLS3il48g4pyYSM6sY2tlxqbinJgg4pePLS3inKtfNDQ1RUJDMjc=	☆--● ✘HáckeR✘ ●--☆_445EBC27	0.6.4
41.35.161.186	1177	Cairo, Egypt	WFhYWFhYWFhYWFhYWFhYWFhYX0U2NTYxNkEz	XXXXXXXXXXXXXXXXXXXX_E65616A3	0.5.0E
41.35.182.232	1177	Alexandria, Egypt	WFhYWFhYWFhYWFhYWFhYWFhYX0JDMkY0NjY5	XXXXXXXXXXXXXXXXXXXX_BC2F4669	0.5.0E
41.35.193.145	1177	Mansoura, Egypt	WFhYWFhYWFhYWFhYWFhYWFhYXzVFRUQyREY5	XXXXXXXXXXXXXXXXXXXX_5EED2DF9	0.5.0E
46.20.37.177	1177	Germany	RGVhZGx5IEhhY2tlcl9CMEM3MkY5MA==	Deadly Hacker_B0C72F90	0.6.4
5.0.236.136	1177	Syrian Arab Republic	SGFjS2VkX0E2OTlERTU4	HacKed_A699DE58	0.5.0E
5.0.42.144	1177	Syrian Arab Republic	aGhoaGhoaGhoaWtra2traywsX0ZDQUZDNDBF	hhhhhhhhhhikkkkkk, ,_FCAFC40E	0.6.4
5.21.235.105	1177	Oman	amVuc2lpaV8xQzAyQUNBNQ==	jensiii_1C02ACA5	0.5.0E
5.245.30.151	1177	Saudi Arabia	2LPZgNmA2YDZgNmA2YDZgNmE2KfZhSBA	ـــــلام @@_C6F05B1E	0.5.0E

			QF9DNkYwNUIxRQ==		
77.30.214.106	87	Riyadh, Saudi Arabia	bW9oYW1tYWRfQUUyMDAwMkU=	mohammad_AE20002E	0.5.0E
78.155.90.73	1177	Syrian Arab Republic	Vi5JLlBfNDY1NTFCNTg=	V.I.P_46551B58	0.5.0E
79.124.66.146	1177	Bulgaria	SGFjXzZFREVEODc5	Hac_6EDED879	0.6.4
79.124.66.148	1177	Bulgaria	SGFjXzZFREVEODc5	Hac_6EDED879	0.6.4
79.124.66.177	1177	Bulgaria	SGFjXzZFREVEODc5	Hac_6EDED879	0.6.4
79.124.66.197	1177	Bulgaria	SGFjXzZFREVEODc5	Hac_6EDED879	0.6.4
79.124.66.200	1177	Bulgaria	SGFjXzZFREVEODc5	Hac_6EDED879	0.6.4
79.124.66.205	1177	Bulgaria	SGFjXzZFREVEODc5	Hac_6EDED879	0.6.4
90.148.71.207	1177	Mecca, Saudi Arabia	NjRfNkMyRUJEMkY=	64_6C2EBD2F	0.5.0E
90.153.166.68	1177	Syrian Arab Republic	SGFjS2VkX0FFNTE5NUVB	HacKed_AE5195EA	0.3.6
90.153.204.11	1177	Syrian Arab Republic	SGFjS2VkX0FFNTE5NUVB	HacKed_AE5195EA	0.3.6
90.153.205.21	1177	Syrian Arab Republic	SGFjS2VkXzU0OTQ2OTJB	HacKed_5494692A	0.3.6
91.140.142.16	1177	Kuwait, Kuwait	SGFjS2VkXzg4NzQ4OTgz	HacKed_88748983	0.6.4
94.203.114.61	1177	Dubai, United Arab Emirates	TWF2ZVJpY2tfRUNEOTRBNUI=	MaveRick_ECD94A5B	0.6.4
94.249.67.47	1177	Amman, Jordan	SGFjS2VkX0RFNkEyMENB	HacKed_DE6A20CA	0.6.4
94.249.69.118	1177	Amman, Jordan	SGFjS2VkXzI0MzMzRDZC	HacKed_24333D6B	0.6.4

** The Base64 encoded data can be observed in the network traffic*

The Fidelis Take

It's clear from this paper that there continues to be considerable global activity involving threat actors using njRAT and associated tools. We're publishing these indicators so that others in the security research community can monitor for this activity and potentially correlate against other campaigns and tools that are being investigated.

Fidelis XPS™ detects all of the activity documented in this paper. The Fidelis Threat Research Team will continue to actively monitor the ever-evolving threat landscape for the latest threats to our customers' security.