THREATS & DEFENSES

Iranian PupyRAT Bites Middle Eastern Organizations

Customized phishing lures distribute PupyRAT malware

WEDNESDAY, FEBRUARY 15, 2017
BY: COUNTER THREAT UNIT RESEARCH TEAM

SecureWorks® Counter Threat Unit™ (CTU) researchers analyzed a phishing campaign that targeted a Middle Eastern organization in early January 2017. Some of messages were sent from legitimate email addresses belonging to several Middle Eastern organizations.

Campaign details

The threat actor used shortened URLs in the body of the phishing emails that redirected to several spoofed domains (See Table 1).

Spoofed domain	Legitimate domain	Associated organization
ntg-sa . com	ntg . com . sa	National Technology Group, a Saudi Arabian telecommunications company
itworx . com-ho . me	itworx . com	ITWorx, an Egyptian information technology services firm
mci . com-ho . me	mci . gov . sa	Saudi Ministry of Commerce
moh . com-ho . me	moh . gov . sa	Saudi Ministry of Health

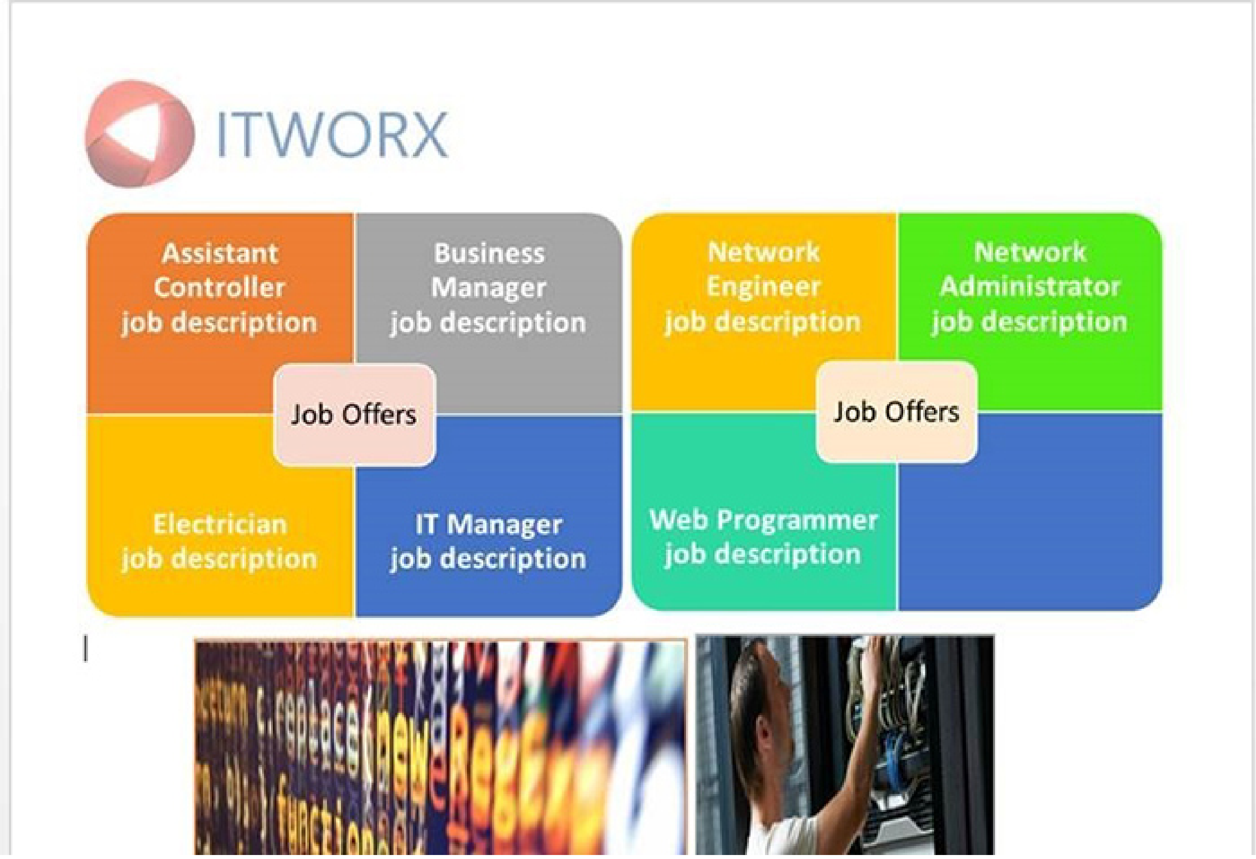
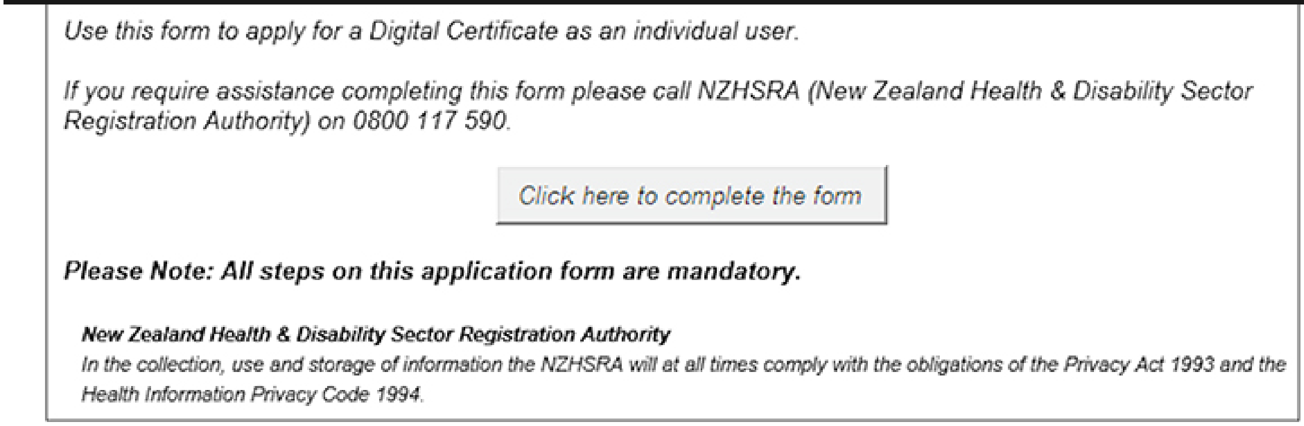

ITWORX
Assistant Controller job description
Business Manager job description
Job Offers
Electrician job description
IT Manager job description
Network Engineer job description
Network Administrator job description
Job Offers
Web Programmer job description

Figure 1. Job offer lure (MD5: 43fad2d62bc23ffdc6d301571135222c). (Source: SecureWorks)



Use this form to apply for a Digital Certificate as an individual user.

If you require assistance completing this form please call NZHSRA (New Zealand Health & Disability Sector Registration Authority) on 0800 117 590.

Please Note: All steps on this application form are mandatory.

New Zealand Health & Disability Sector Registration Authority
In the collection, use and storage of information the NZHSRA will at all times comply with the obligations of the Privacy Act 1993 and the Health Information Privacy Code 1994.

Figure 2. Ministry of Health lure (MD5: 1b5e33e5a244d2d67d7a09c4ccf16e56). (Source: SecureWorks)

The downloaded document attempts to run a macro that then runs a PowerShell command. This command downloads two additional PowerShell scripts that install PupyRAT, an open-source remote access trojan (RAT). According to the developer, PupyRAT is a “multi-platform (Windows, Linux, OSX, Android), multi-function RAT and post-exploitation tool mainly written in Python.” CTU™ analysis confirms that PupyRAT can give the threat actor full access to the victim's system.

Conclusion

CTU analysis suggests this activity is related to Iranian threat actors closely aligned with or acting on behalf of the COBALT GYPSY threat group (formerly labeled Threat Group-2889). CTU researchers assess with high confidence that COBALT GYPSY is associated with Iranian government-directed cyber operations, and it has used tactics similar to this campaign:

- targeting Saudi financial, oil, and technology organizations
- using job-themed lures to infect systems
- registering spoofed domains
- spearphishing new victims using legitimate email addresses

This campaign highlights the need for organizations to educate users about the risks of spearphishing and shortened links. CTU researchers recommend that organizations disable macros in Microsoft Office products to prevent attacks that leverage this functionality.

domains may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
ntg-sa . com	Domain name	Attacker-controlled spoofed website
itworx . com-ho . me	Domain name	Attacker-controlled spoofed website
mci . com-ho . me	Domain name	Attacker-controlled spoofed website
moh . com-ho . me	Domain name	Attacker-controlled spoofed website
mol . com-ho . me	Domain name	Attacker-controlled spoofed website
45 . 32 . 186 . 33	IP address	Hosting spoofed domains used in PupyRAT phishing campaign
139 . 59 . 46 . 154	IP Address	Hosting PowerShell stages of PupyRAT download
89 . 107 . 62 . 39	IP Address	PupyRAT command and control server
43fad2d62bc23ffdc6d301571135222c	MD5 hash	Job-themed Word document lure (qhtma) delivering PupyRAT
735f5d7ef0c5129f0574bec3cf3d6b06b052744a	SHA1 hash	Job-themed Word document lure (qhtma) delivering PupyRAT
e5b643cb6ec30d0d0b458e3f2800609f260a5f15c4ac66faf4ebf384f7976df6	SHA256 hash	Job-themed Word document lure (qhtma) delivering PupyRAT
1b5e33e5a244d2d67d7a09c4ccf16e56	MD5 hash	Ministry of Health lure (Health_insurance_registration.doc) delivering PupyRAT
934c51ff1ea00af2cb3b8465f0a3effcf759d866	SHA1 hash	Ministry of Health lure (Health_insurance_registration.doc) delivering PupyRAT
66d24a529308d8ab7b27ddd43a6	SHA256	Ministry of Health lure

ea546c794e57b		(Password_Policy.xlsm) delivering PupyRAT
6c195ea18c05bbf091f09873ed9cd533ec7c8de7a831b85690e48290b579634b	SHA256 hash	Password-themed lure (Password_Policy.xlsm) delivering PupyRAT
97cb7dc1395918c2f3018c109ab4ea5b	MD5 hash	PupyRAT (pupyx86.dll)
3215021976b933ff76ce3436e828286e124e2527	SHA1 hash	PupyRAT (pupyx86.dll)
8d89f53b0a6558d6bb9cdbc9f218ef699f3c87dd06bc03dd042290dedc18cb71	SHA256 hash	PupyRAT (pupyx86.dll)

Table 2. Threat indicators for the Iranian PupyRAT campaign.

Gauging confidence level

CTU researchers have adopted the grading system published by the U.S. Office of the Director of National Intelligence to indicate confidence in their assessments:

- High confidence generally indicates that judgments are based on high-quality information, and/or that the nature of the issue makes it possible to render a solid judgment. A "high confidence" judgment is not a fact or a certainty, however, and such judgments still carry a risk of being wrong.
- Moderate confidence generally means that the information is credibly sourced and plausible but not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.
- Low confidence generally means that the information's credibility and/or plausibility is questionable, or that the information is too fragmented or poorly corroborated to make solid analytic inferences, or that [there are] significant concerns or problems with the sources.

Tags: **PUPYRAT** **THREAT INTELLIGENCE**

RELATED CONTENT