

RSA®Conference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

SESSION ID: PART1-T10

Inside the Takedown of the Rubella Macro Builder Suspect



John Fokker

Head of Cyber Investigations, Principal Engineer

McAfee

@john_fokker

#RSAC

Speaker



John Fokker

Head of Cyber Investigations, Principal Engineer

McAfee ATR team

@John_Fokker

RSA®Conference2020

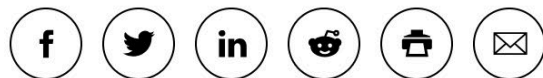
What is a Macro Builder?

And why should McAfee care...

Rubella Macro Builder cybercrimeware kit receives lower price, new capabilities

Doug Olenick Online Editor

[Follow @DougOlenick](#)



Gootkit

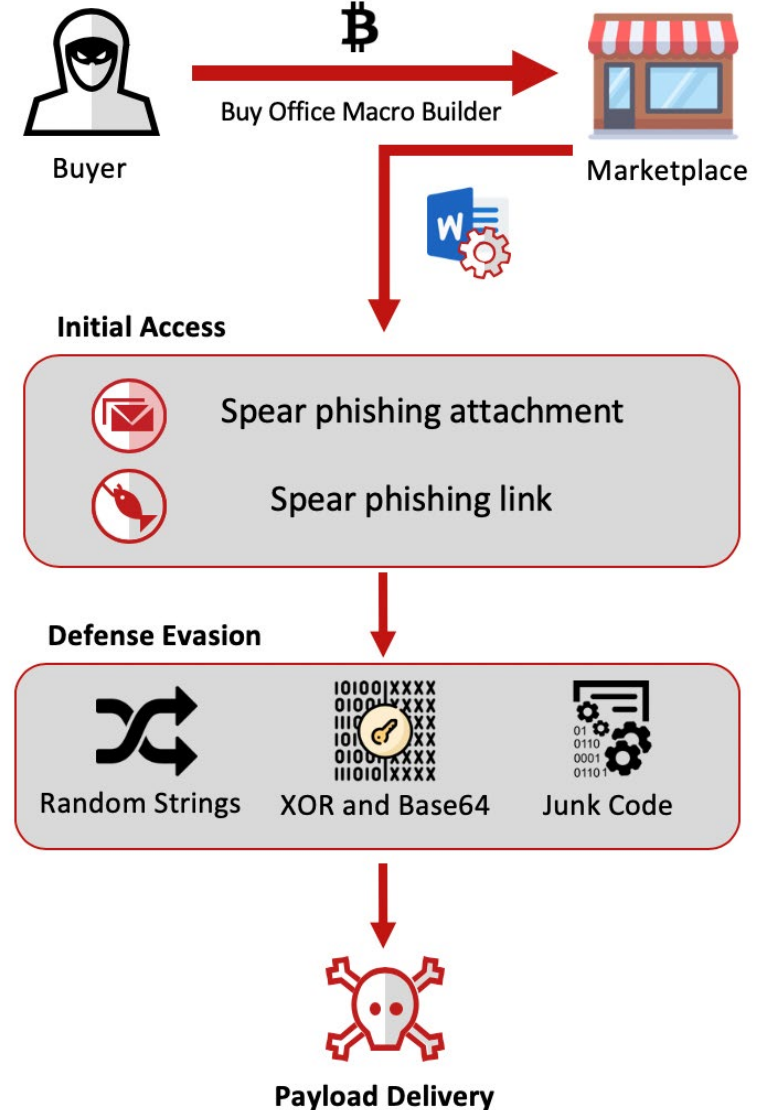
Russian hackers have taken a shine to a new

cybercrimeware kit called Rubella Macro Builder that is being touted as fast, cheap and capable of beating a basic antivirus defensive system.

What is a Macro Builder?

- Specialized toolkit to weaponize MS office documents
- Outsourcing Expertise
 - Macro building
 - Obfuscation
 - AMSI evasion
- Facilitating (Spear)phishing on a larger scale.
- Middle-man function

Office Macro Builder Overview



MITRE ATTACK Techniques of Threats against Retail

mitre-mobile-attack	mitre-attack	mitre-pre-attack	0 1 2 3 4 5 6 7 8 9 Show a								
Initial access (11 items)	Execution (34 items)	Persistence (63 items)	Privilege escalation (32 items)	Defense evasion (74 items)	Credential access (24 items)	Discovery (25 items)	Lateral movement (21 items)	Collection (14 items)	Command and control (22 items)	Exfiltration (10 items)	Impact (16 items)
Spearphishing Attachment	User Execution	Scheduled Task	Scheduled Task	Obfuscated Files or Information	Credential Dumping	System Information Discovery	Remote File Copy	Automated Collection	Commonly Used Port	Automated Exfiltration	Data Encrypted for Impact
Spearphishing Link	PowerShell	New Service	New Service	Scripting	Account Manipulation	Account Discovery	Pass the Hash	Email Collection	Standard Application Layer Protocol	Exfiltration Over Command and Control Channel	System Shutdown/Reboot
Valid Accounts	Scripting	Registry Run Keys / Startup Folder	Process Injection	Deobfuscate/Decode Files or Information	Brute Force	Permission Groups Discovery	Remote Desktop Protocol	Input Capture	Data Encoding	Data Encrypted	Account Access Removal
Drive-by Compromise	Scheduled Task	Account Manipulation	Access Token Manipulation	Modify Registry	Credentials from Web Browsers	Process Discovery	AppleScript	Clipboard Data	Connection Proxy	Exfiltration Over Alternative Protocol	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Create Account	DLL Search Order Hijacking	Mshta	Hooking	Domain Trust Discovery	Application Access Token	Data Staged	Remote Access Tools	Data Compressed	Defacement
External Remote Services	Mshta	DLL Search Order Hijacking	Hooking	Code Signing	Input Capture	File and Directory Discovery	Application Deployment Software	Data from Information Repositories	Remote File Copy	Data Transfer Size Limits	Disk Content Wipe
Supply Chain Compromise	Rundll32	Hooking	Startup Items	Disabling Security Tools	Private Keys	Virtualization/Sandbox Evasion	Component Object Model and Distributed COM	Data from Local System	Uncommonly Used Port	Exfiltration Over Other Network Medium	Disk Structure Wipe
Trusted Relationship	Execution through API	Startup Items	Valid Accounts	Connection Proxy	Credentials in Files	Network Sniffing	Distributed Component Object Model	Screen Capture	Web Service	Exfiltration Over Physical Medium	Endpoint Denial of Service
Hardware Additions	Execution through Module Load	Valid Accounts	Accessibility Features	File Deletion	Network Sniffing	Query Registry	Exploitation of Remote Services	Audio Capture	Data Obfuscation	Scheduled Transfer	Firmware Corruption
Replication Through Removable Media	Exploitation for Client Execution	Accessibility Features	Application Shimming	Process Injection	Bash History	Security Software Discovery	Internal Spearphishing	Data from Cloud Storage Object	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Spearphishing via Service	Windows Management Instrumentation	Application Shimming	Bypass User Account Control	Rundll32	Cloud Instance Metadata API	System Network Configuration Discovery	Logon Scripts	Data from Network Shared Drive	Standard Non-Application Layer Protocol		Network Denial of Service
	Compiled HTML File	Bootkit	Exploitation for Privilege Escalation	Web Service	Credentials in Registry	System Network Connections Discovery	Pass the Ticket	Data from Removable Media	Custom Command and Control Protocol		Resource Hijacking
	Graphical User	Browser Extensions	Path Interception	Access Token	Exploitation for	System Owner/User	Remote Services	Man in the Browser	Domain Generation		Runtime Data

RSA[®]Conference2020

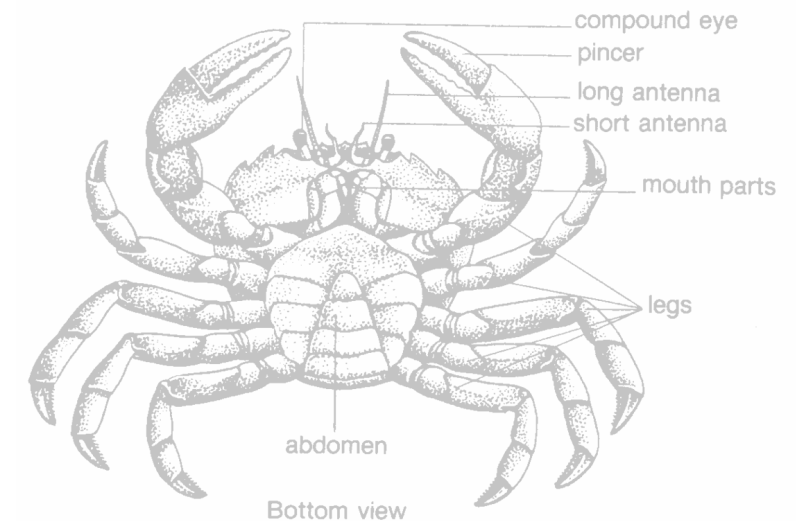
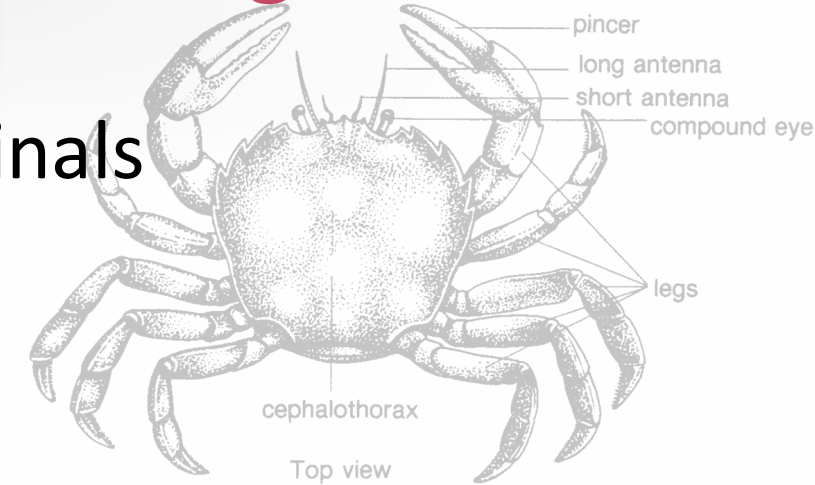
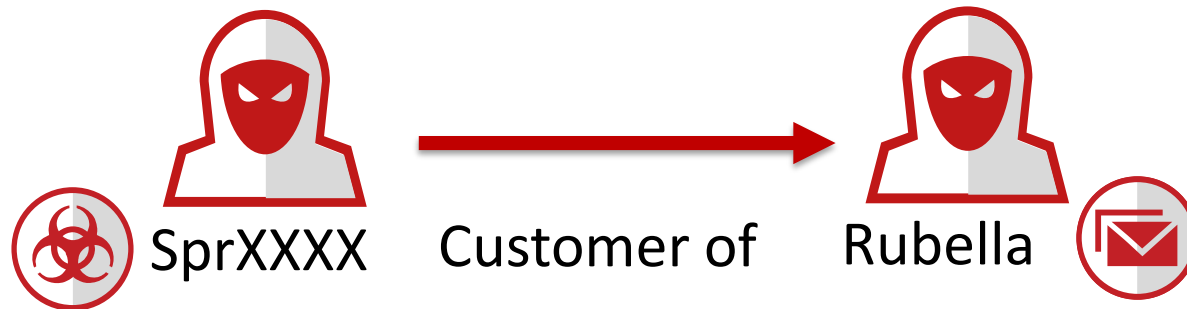
How did it start for us? :


Hunting for Gandcrab Ransomware but catching Rubella...

Linking the adversary to their tools


Hunting for Gandcrab ransomware but catching Rubella...

- Looking at relationships between cybercriminals on Cyber criminal forums
- Affiliates research of Gandcrab ransomware
- One particular affiliate was a user of the Rubella Macro Builder





[ПРОФИЛЬ](#)
[ПМ](#)

[ЖАЛОБА](#)
[ВВЕРХ](#)

Rubella 


5.11.2018, 20:28

Finally, bypassed f...g AMSI...
<http://prntscr.com/leqgz4>

гигабайт


Группа: [Seller](#)
 Сообщений: 143
 Регистрация: 20.02.2018
 Из: Mordor
 Пользователь №: 85 692
 Деятельность: [КОДИНГ](#)


Репутация: [4](#)
 (0% - хорошо)


[ПРОФИЛЬ](#)
[ПМ](#)

[ЖАЛОБА](#)
[ВВЕРХ](#)

spr

Сегодня, 10:06

байт


Группа: Пользователь
 Сообщений: 4
 Регистрация: 23.02.2018
 Пользователь №: 85 767
 Деятельность: [другое](#)

Репутация: [1](#)
 (0% - хорошо)

Цитата(Rubella @ 5.11.2018, 22:28)

Finally, bypassed f...g AMSI...
<http://prntscr.com/leqgz4>

reply jabber dude..



Rubella



SprXXXX



MS Office version in Dutch

giovanni (Compatibiliteitsmodus) - Word

Aanmelden

Indeling Verwijzingen Verzendlijsten Controleren Beeld Ontwikkelaars Help Uitleg Delen

Stijlen Bewerken

PuTTY Configuration

Category:

- Session
 - Logging
- Terminal
 - Keyboard
 - Bell
- Features
- Window
 - Appearance
 - Behaviour
 - Translation
 - Selection
 - Colours
- Connection
 - Data
 - Proxy
 - Telnet
 - Rlogin
 - SSH
 - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) Port

public 22

Connection type:

☐ Raw ☐ Telnet ☐ Rlogin ☒ SSH ☐ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Load Save Delete

Close window on exit:

☐ Always ☐ Never ☒ Only on clean exit

About Open Cancel

14 items 1 item selected 80.0 KB

Windows Defender

PC status: Potentially unprotected

Home Update History

Virus and spyware definitions: Up to date

Your virus and spyware definitions are automatically updated to help protect your PC.

Definitions created on:	11/5/2018 at 8:01 AM
Definitions last updated:	11/5/2018 at 11:21 AM
Virus definition version:	1.279.1245.0
Spyware definition version:	1.279.1245.0

Update

Did you know?

Virus, spyware, and other malware definitions are files that are used to identify malicious or potentially harmful software on your PC. These definitions are updated automatically, but you can also click Update to get the latest definitions you want.

WHY WOULD YOU USE RUBELLA?



The macro has been FUD for 4 weeks already and has the longest FUD times on the market.



Has many options to customize your output



Can be attached in GMAIL



A limit of 10 customs makes sure that it will stay undetected for a longer period of time.

500\$/MONTH

This includes 10 reFUDs (more than you will ever need) and complete customer support

THE ONLY PAYMENT METHOD IS BITCOIN (BTC)

If you'd like to purchase Rubella or ask me a question about the product, you can contact me on jabber.

Rubella@exploit.im

TERMS OF SERVICE

- Do not try to crack, leak, reverse engineer or anything which does not seem appropriate to Rubella Builder.
- Reselling/sharing of macros generated by your Rubella builder is strictly forbidden.
- You are not allowed share your license. One license is for one customer.
- Rubella is a pentesting tool. I am not responsible for anything you do using Rubella.

So who is Rubella?

- Postings
 - A seller on the Notorious Exploit forum.
- Interests
 - Tantalus Ransomware-as-a-Service
 - Goliath Loader, 2nd stage Implants
 - Havana Cryptowallet stealers
 - Stolen Credit card and Gift cards
 - Email spoofing software
- Monikers (new and old) going back to 2014
 - Rubella, KiXXX, codXXX, MarXXXX

[Coming Soon] Goliath Loader, GoliathLoader will be for rent soon.

Подписка на тему | Версия для печати

Rubella 1.04.2018, 20:19

Hello all,

гигабайт

Группа: **Seller**
Сообщений: 143
Регистрация: 20.02.2018
Из: Mordor
Пользователь №: 85 692
Деятельность: **коддинг**

Репутация: 4
(0% - хорошо)

I have been running my macrobuilder project for around 7 weeks now on here, and I have had many good results with results: it has been FUD now for **7 weeks**.

This is why I decided that I would create a new product. As you might know, I want to deliver quality. My macrobuilder will do the same thing with Goliath. I will rent it to 6-10 people (I will decide on this later, I think there will be more people interested in it)

Features:
-Coded in C (no dependencies, fully native).

Havana Stealer [C] [75\$], Selling crypto wallet replacer

Подписка на тему | Версия для печати

Rubella 6.05.2018, 19:34

гигабайт

Группа: **Seller**
Сообщений: 143
Регистрация: 20.02.2018
Из: Mordor
Пользователь №: 85 692

Havana Crypto Wallet Replacer

Functions:
-FUD scantime & runtime
-Coded in pure C from scratch
-5kb file
-No dependencies

Release [FREE] E-mail Spoofer

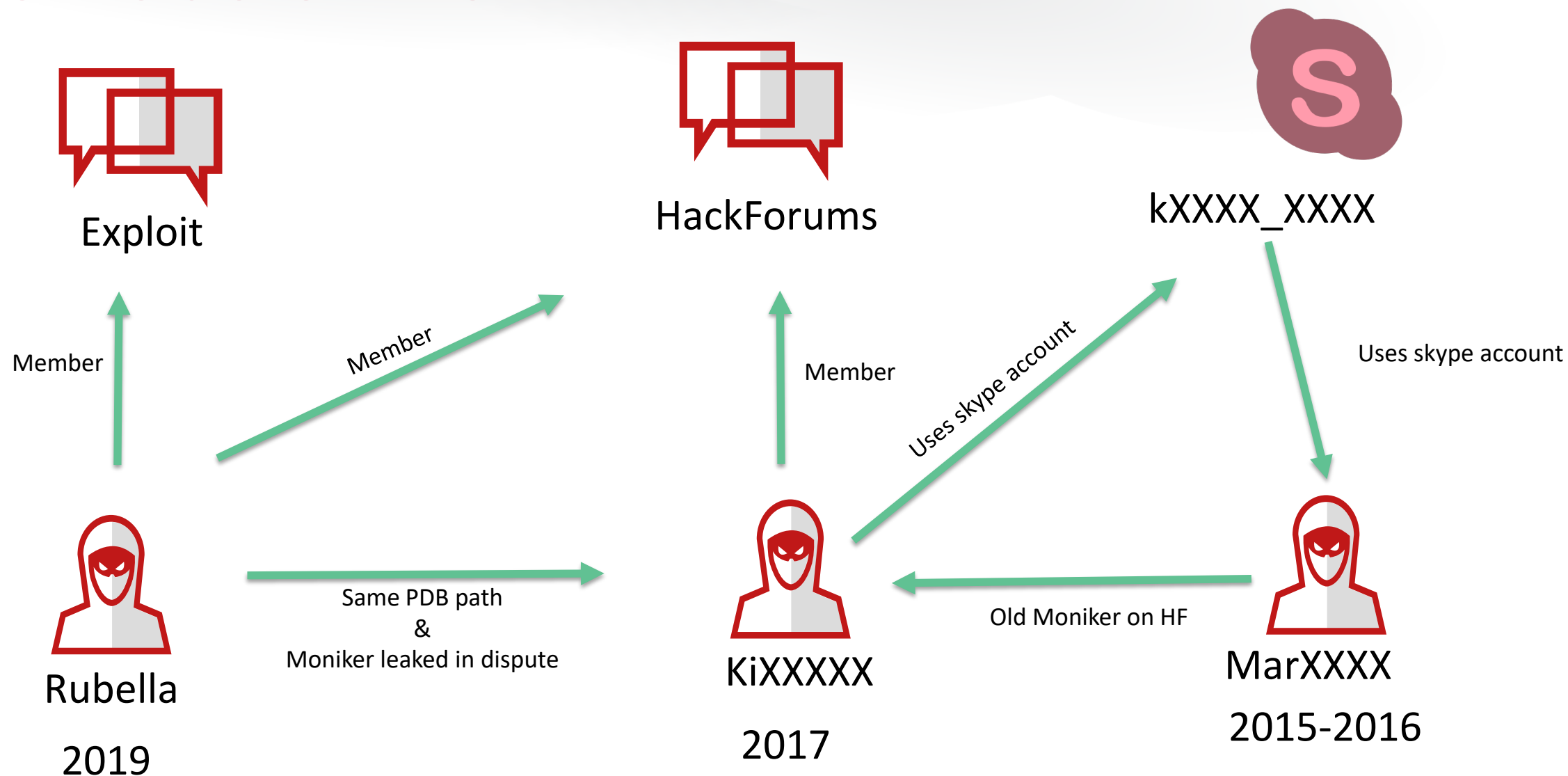
02-19-2018, 05:30 PM (This post was last modified: 02-19-2018, 05:52 PM by Rubella)

Just coded this e-mail spoofer and thought I'd release it for free. You can use it to change the name to anything you like and hit inbox. For example, you could use it to make it look like it's from a friend. It will work. Can be nice if you want to fool with someone.


Rubella •
XMPP: Rubella@exploit.im

-Coded in C#
-Send to multiple e-mails at once
-Spoof the e-mail displayed
-Hit inbox (without attachments)
-Possibility to add an attachment

Monikers over time...



Climbing the Criminal Career Ladder



Forum menu

Forum > TV





RUBELLA

Rubella is without a doubt the most advanced macro-builder on the market. It features many different options, allowing you to generate a completely unique and FUD .XLS/DOC file whenever you need one. No more waiting for the coder to clean the macro every day. With Rubella, you will be able to spread for weeks without it getting detected. It has been undetected for 4 weeks as of now and is still going strong.

FEATURES

- ✓ .XLS and .DOC output files (Excel and Word)
- ✓ Option for custom powershell payload (one-liner)
- ✓ Ability to add decoy text which will appear when the victim enables the macro
- ✓ Generate unique and randomly placed junkcode (for AV evasion & uniqueness)
- ✓ Different encryption methods (BASE64 and XOR)
- ✓ Choose between AutoOpen() and AutoClose() macro methods
- ✓ Ability to add a custom picture from the internet (by URL) which will be loaded when the macro gets enabled
- ✓ Generate unique and randomly placed logos (for AV evasion & uniqueness)
- ✓ Proper licensing/login system which uses credentials and a hardware ID
- ✓ Different download methods (PowerShell, Bitadmin, Microsoft.XMLHTTP, MDXML2.XMLHTTP)
- ✓ Ability to add a custom template which will disappear once the victim enables the macro
- ✓ Choose a name for the dropped file
- ✓ Every generated macro is unique to bypass static analysis

WHY WOULD YOU USE RUBELLA?

- The macro has been FUD for 4 weeks already and has the longest FUD times on the market.
- Can be attached in GMAIL.
- Has many options to customize your output
- A limit of 10 customs makes sure that it will stay undetected for a longer period of time.

500\$/MONTH

This includes 10 reFUDs (more than you will ever need) and complete customer support

THE ONLY PAYMENT METHOD IS BITCOIN (BTC)

If you'd like to purchase Rubella or ask me a question about the product, you can contact me on jabber.

Rubella@exploit.im

TERMS OF SERVICE

- Do not try to crack, leak, reverse engineer or anything which does not seem appropriate to Rubella Builder.
- Reselling/sharing of macros generated by your Rubella builder is strictly forbidden.
- You are not allowed share your license. One license is for one customer.
- Rubella is a pen-testing tool. I am not responsible for anything you do using Rubella.

Upon breaking one or more of the above-mentioned rules, I reserve the right to terminate your license and blacklist you from my service at any time.

This product is meant for pen-testing and I am not responsible for any malicious use of this tool. Do not break the laws of your country using this tool, if you do then solely you are responsible.

RSA[®]Conference2020

Working the Human element

“Mister Rubella, Is there anything else you would like to add yourself?”

Meet John Doe

- John is your average SYS Admin
- John got fired recently by company X
- Not a coder nor a skilled hacker
- But... John holds a grudge.. 😞
 - Looking for a Macro Builder and RAT tool to infect his former employer.

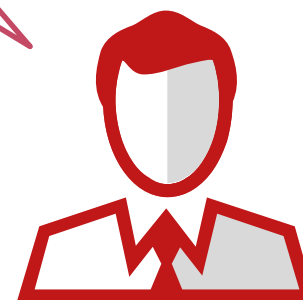


Hi

Hi, I saw your stuff
online, pretty cool



Rubella



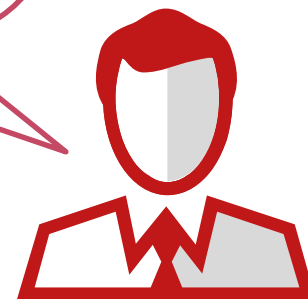
John Doe

how can i help?



Rubella

I was looking online for a word macro builder and I found your postings. It seems pretty cool, so that is why I added you to my contacts, might come in handy



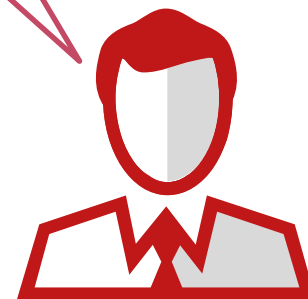
John Doe

Okay good
you wish to buy



Rubella

Maybe, but I have to
work on my payload



John Doe

Dryad Macro Builder

Main

Decoy Options

Anti-Virus Evasion

Script Generator

Generate Macro

Payload Options

Payload URL:

Macro mode:

Download Method:

Payload type:

Drop name:

Stub

Stub path:

Output format

☐ Microsoft Word (.doc)

☒ Microsoft Excel (.xls)



Rubella





RUBELLA

Rubella is without a doubt the most advanced macro-builder on the market. It features many different options, allowing you to generate a completely unique and FUD XLS/DOC file whenever you need one. No more waiting for the coder to clean the macro every day. With Rubella, you will be able to spread for weeks without it getting detected. It has been undetected for 4 weeks as of now and is still going strong.

FEATURES

- ☒ XLS and DOC output files (Excel and Word)
- ☒ Different encryption methods (BASE64 and XOR)
- ☒ Different download methods (PowerShell, Bitadmin, Microsoft.XMLHTTP, MSXML2.XMLHTTP)
- ☒ Option for custom powershell payload (one-liner)
- ☒ Choose between AutoOpen() and AutoClose() macro methods
- ☒ Ability to add a custom template which will disappear once the victim enables the macro
- ☒ Ability to add decoy text which will appear when the victim enables the macro
- ☒ Ability to add a custom picture from the internet (by URL) which will be loaded when the macro gets enabled.
- ☒ Choose a name for the dropped file
- ☒ Generate unique and randomly placed junkcode (for AV evasion & uniqueness)
- ☒ -Generate unique and randomly placed loops (for AV evasion & uniqueness)
- ☒ Every generated macro is unique to bypass static analysis
- ☒ Proper licensing/login system which uses credentials and a hardware ID

WHY WOULD YOU USE RUBELLA?

-  The macro has been FUD for 4 weeks already and has the longest FUD times on the market.
-  Has many options to customize your output
-  Can be attached in GMAIL
-  A limit of 10 customs makes sure that it will stay undetected for a longer period of time.

500\$/MONTH

This includes 10 reFUDs (more than you will ever need) and complete customer support

THE ONLY PAYMENT METHOD IS BITCOIN (BTC)

If you'd like to purchase Rubella or ask me a question about the product, you can contact me on jabber.

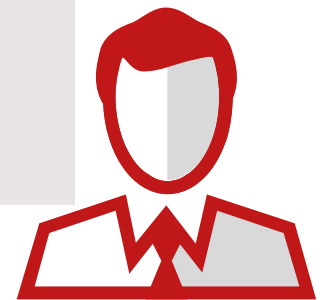
Rubella@exploit.im

TERMS OF SERVICE

- Do not try to crack, leak, reverse engineer or anything which does not seem appropriate to Rubella Builder.
- Reselling/sharing of macros generated by your Rubella builder is strictly forbidden.
- You are not allowed share your license. One license is for one customer.
- Rubella is a pentesting tool. I am not responsible for anything you do using Rubella.

Upon breaking one or more of the abovementioned rules, I reserve the right to terminate your license and blacklist you from my service at any time.

This product is meant for pentesting and I am not responsible for any malicious use of this tool. Do not break the laws of your country using this tool, if you do then solely you are responsible.



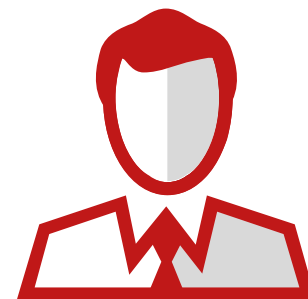
John Doe

Its different product
But its better than
Rubella



Rubella

Dryad?
Ok. Don't mind me
asking why did you
change the name?
or is it totally
different?



John Doe

Ofcourse!

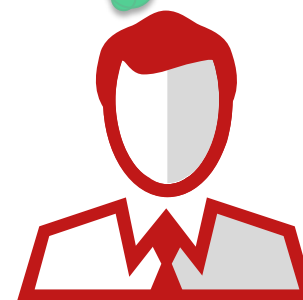
oh wow, you built all
this yourself?

Confession!!

Thank You



Rubella



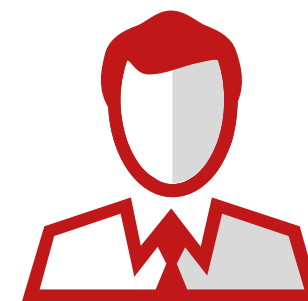
John Doe

Not really, But I can offer to code a custom bot but it would take some time and it would require a pretty big budget
For private bot in C



Rubella

cool!! I am looking for a good RAT tool as payload, do you have any advice?



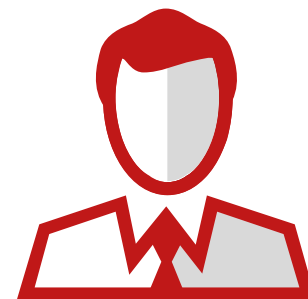
John Doe

Yes NP.

Interesting maybe
if I have some
more money....



Rubella



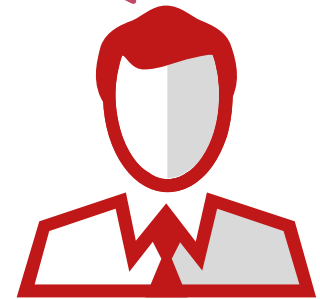
John Doe



Rubella

Dont
know
Different
times

Thank you so much
already, been great
chatting . I am certainly
interested
When are you online if I
want reach out again?



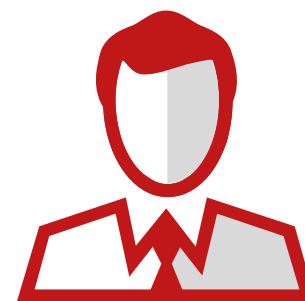
John Doe



Rubella

cy
cya

k
c u later



John Doe

RSA®Conference2020

Technical analysis of the Rubella and Dryad Macro Builder

How does it work under the hood

Classic Mistakes...

The screenshot displays the VT Intelligence web interface for a file analysis. The file ID is 77230f7d3a738aba833c3fcb03fb3b9953f9410107ed8df527dfd9098ac59dfc. The file is named 'Spoofers.exe', is 15 KB, and was analyzed on 2018-03-19 18:20:42 UTC. A red warning indicates that one engine detected the file as malicious. The file is a Win32 EXE, PE32 executable for MS Windows (GUI) Intel 80386 Mono/.Net assembly.

The interface includes tabs for DETECTION, DETAILS, BEHAVIOR, CONTENT, SUBMISSIONS, and COMMUNITY. The DETAILS tab is active, showing Basic Properties, Names, Signature Info, Signature Verification, File Version Information, Tags, History, .NET Details, Portable Executable Info, and Debug Artifacts.

Basic Properties

MD5	347564260e576aec8496876f57761d50
SHA-1	5f699ca93aac133636ad7060299fd9fd3754e815
Authentihash	86787d2638d9b61feb5530d82d73f297a502c93c60eab1c9bdc9fc242b3bb403
Imphash	f34d5f2d4577ed6d9ceec516c1f5a744
SSDEEP	384:19sK6thpmhuUUICOnm6dC6WaUrGVQAijm1td3sR:IKTUlrw6OjtsR
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 Mono/.Net assembly
File size	15 KB

Names

Spoofers.exe

Signature Info

Signature Verification

File is not signed

File Version Information

Copyright Copyright © 2018

Tags

assembly peexe

History

Creation Time	2018-02-19 16:48:33
First Submission	2018-02-19 16:50:35
Last Submission	2018-02-19 16:50:35
Last Analysis	2018-03-19 18:20:42
Debug Artifacts	2018-02-19 15:48:33

.NET Details

Module Version Id	9af8e573-fe68-4bdb-b98e-0dbaf70a661b
TypeLib Id	2ba966a4-5c33-4b38-94dc-a4501ea42959

Portable Executable Info

Debug Artifacts

Path	C:\Users\Breitling\source\repos\Spoofers\Spoofers\obj\Debug\Spoofers.pdb
GUID	79998673-a2de-49cd-bf01-45724df6db7e

Linking the PDB paths to more Rubella software

VTINTELLIGENCE C:\Users\Breitling*

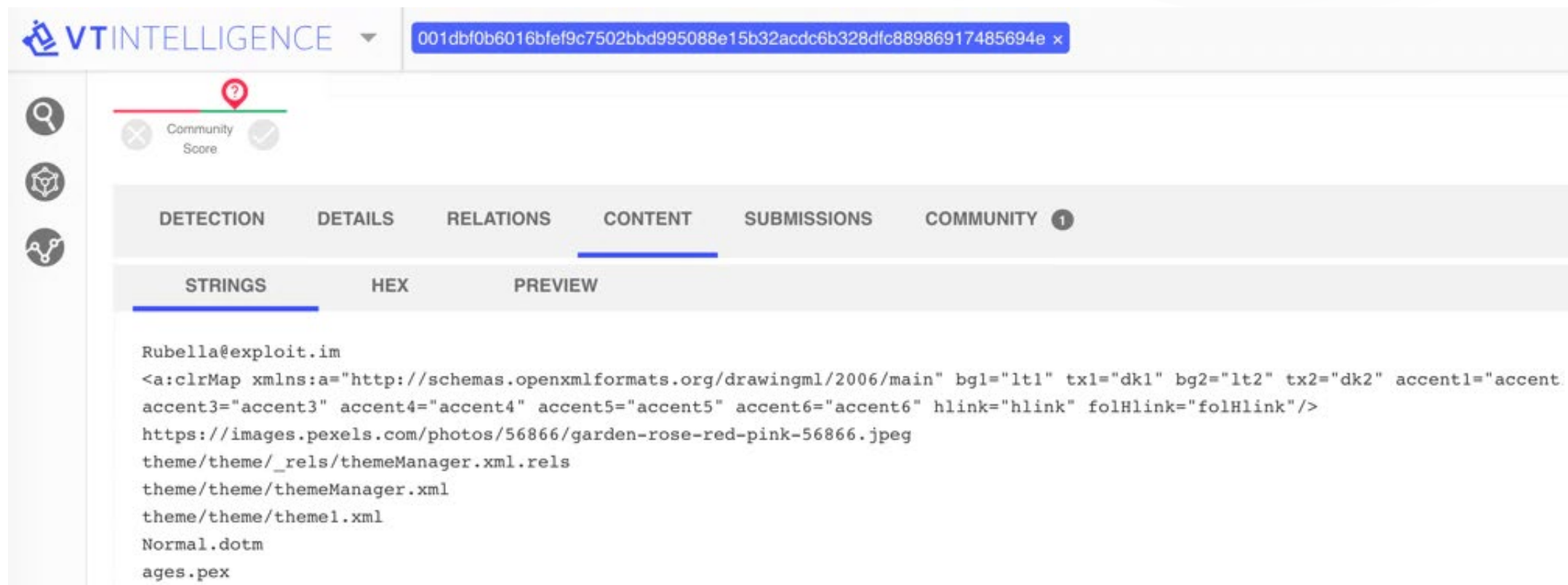
FILES 6	COMMONALITIES
<input type="checkbox"/> b80f73312d00f71b52a51e0d2c49ebe7b12cb24c7b6beab9b0bd4f9e232630e1 Spoof.exe peexe assembly	2 / 64 15 KB 2018-06-02 05:38:42 first seen 2018-06-02 05:38:42 last seen 1 submissions 1 submitters
<input type="checkbox"/> 2a20d3d9ac4dc74e184676710a4165c359a56051c7196ca120cf8716b7c21b9 RubellaBuilder.exe peexe assembly	23 / 66 796.5 KB 2018-03-14 11:31:09 first seen 2018-03-27 01:13:49 last seen 8 submissions 2 submitters
<input type="checkbox"/> 77230f7d3a738aba833c3fcb03fb3b9953f9410107ed8df527dfd9098ac59dfc Spoof.exe peexe assembly	1 / 64 15 KB 2018-02-19 16:50:35 first seen 2018-02-19 16:50:35 last seen 2 submissions 1 submitters
<input type="checkbox"/> 421c8c40a533bd081d9022c1927105e72b9b4c9d0e8b00e781767d55276b5af4 Spoof.exe peexe assembly	1 / 64 15 KB 2018-02-19 16:26:09 first seen 2018-02-19 16:26:09 last seen 2 submissions 1 submitters
<input type="checkbox"/> d67b0e85ef57804a2db6abab2cd990811c20dc0e059e765fb14e4cb3d44b1f6c ...ft\Windows Sidebar\Gadgets\chameleon_digiclock.gadget\Gadget.xml xml	0 / 60 742 B 2013-12-29 14:13:01 first seen 2017-12-02 14:59:09 last seen 2 submissions 2 submitters
<input type="checkbox"/> 2881e98717cd7eaa9b4d6ed4a688f1c68cd252513205e6493911c67425d56da QuickNote_v1.0.exe peexe assembly	0 / 63 176.5 KB 2017-07-05 16:28:22 first seen 2017-07-15 16:05:45 last seen 2 submissions 2 submitters

```
C:\Users\Breitling\Desktop\SamehadaLogger\KServer\KServer\bin\Debug\KServer.exe

>>>Please enter the port for the listener.
1443
Please enter an IP for the listener.
192.168.2.8
A client has connected.
enablerdp
Remote Desktop is now DISABLED
enablerdp
Remote Desktop is now ENABLED
enablerdp
Remote Desktop is now DISABLED
enablerdp
Remote Desktop is now ENABLED

C:\Users\Breitling\Desktop\SamehadaLogger\KServer\KServer\bin\Debug\KServer.exe
```

Some files even included his JabberID



VTINTELLIGENCE

001dbf0b6016bfef9c7502bbd995088e15b32acdc6b328dfc88986917485694e x

Community Score

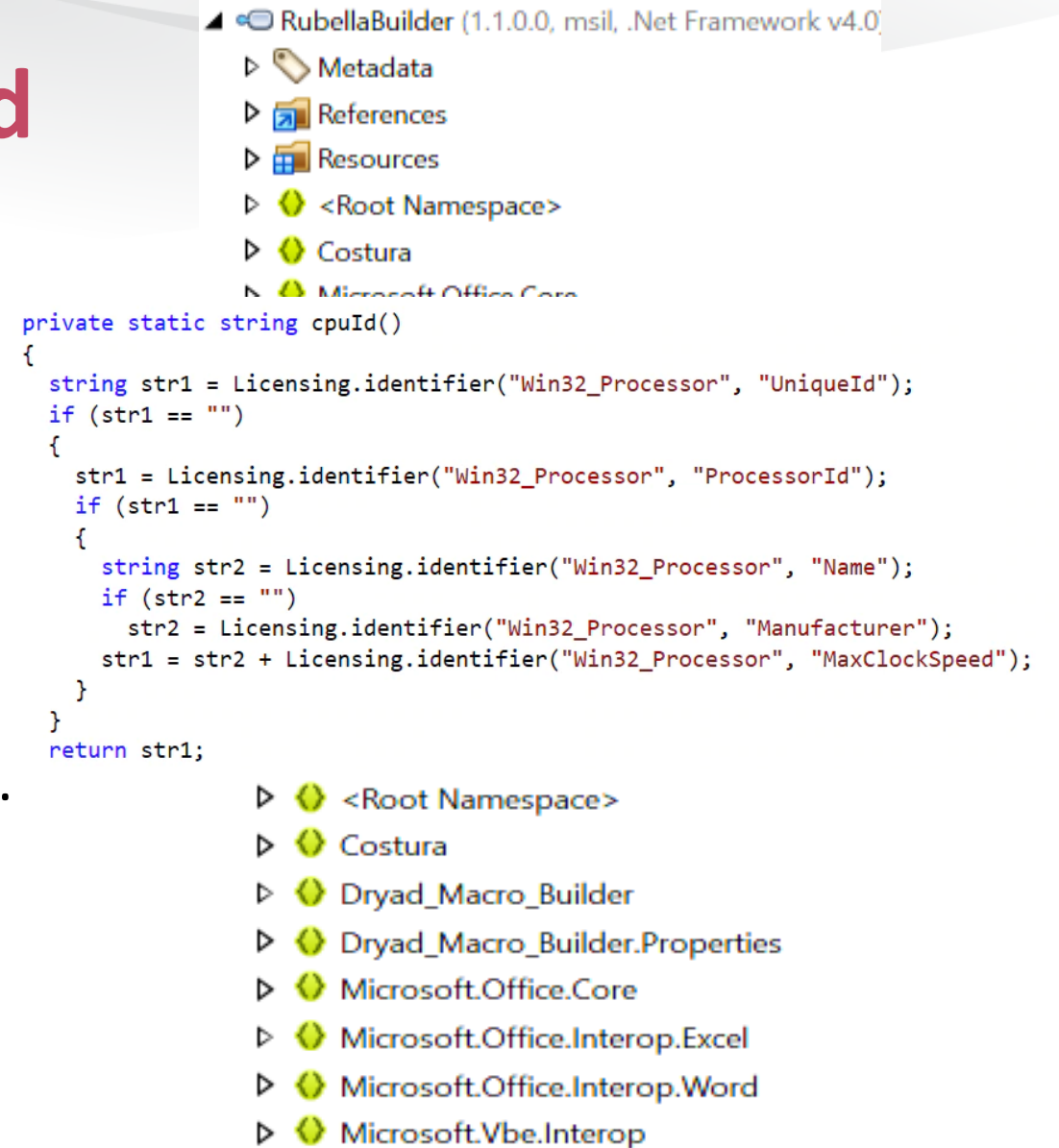
DETECTION DETAILS RELATIONS **CONTENT** SUBMISSIONS COMMUNITY 1

STRINGS HEX PREVIEW

Rubella@exploit.im
<a:clrMap xmlns:a="http://schemas.openxmlformats.org/drawingml/2006/main" bgl="lt1" tx1="dk1" bg2="lt2" tx2="dk2" accent1="accent
accent3="accent3" accent4="accent4" accent5="accent5" accent6="accent6" hlink="hlink" folHlink="folHlink"/>
https://images.pexels.com/photos/56866/garden-rose-red-pink-56866.jpeg
theme/theme/_rels/themeManager.xml.rels
theme/theme/themeManager.xml
theme/theme/theme1.xml
Normal.dotm
ages.pex

Comparing Rubella and Dryad

- Both Kits developed in .Net
- No obfuscation in the actual Toolkit
- A built-in licensing function
- Both Kits have been offered to Malware Ops in order to double check that we offer protection.



```

private static string cpuId()
{
    string str1 = Licensing.identifier("Win32_Processor", "UniqueId");
    if (str1 == "")
    {
        str1 = Licensing.identifier("Win32_Processor", "ProcessorId");
        if (str1 == "")
        {
            string str2 = Licensing.identifier("Win32_Processor", "Name");
            if (str2 == "")
            {
                str2 = Licensing.identifier("Win32_Processor", "Manufacturer");
                str1 = str2 + Licensing.identifier("Win32_Processor", "MaxClockSpeed");
            }
        }
    }
    return str1;
}

```

Project Structure:

- ▶ Metadata
- ▶ References
- ▶ Resources
- ▶ <Root Namespace>
- ▶ Costura
- ▶ Microsoft Office Core

Assembly References:

- ▶ <Root Namespace>
- ▶ Costura
- ▶ Dryad_Macro_Builder
- ▶ Dryad_Macro_Builder.Properties
- ▶ Microsoft.Office.Core
- ▶ Microsoft.Office.Interop.Excel
- ▶ Microsoft.Office.Interop.Word
- ▶ Microsoft.Vbe.Interop

Obfuscation recipe

- Generating Random Strings, Characters and Numbers
- A pinch of Junk Code
- Mixing it all together in a Macro
- Adding the obfuscation recipe to the McAfee detection cookbook

```
internal class JunkCode
{
    public static string Junk1
    {
        string str1 = RanGen.Ran
        string str2 = RanGen.Ran
        RanGen.RandomVariable(ran
        int int32 = Convert.ToInt
        Convert.ToInt32(RanGen.Ri
        Convert.ToInt32(RanGen.Ri
        string macroCode = "" + '
        return WriteMacro.Press(i
    }

    public static string Junk2
    {
        string str1 = RanGen.Ran
        RanGen.RandomVariable(ran
        RanGen.RandomVariable(ran
        Convert.ToInt32(RanGen.Ri
        Convert.ToInt32(RanGen.Ri
        Convert.ToInt32(RanGen.Ri
        string str2 = "";
        if (Convert.ToInt32(RanGe
        {
            str2 = str2 + "Dim " +
            for (int int16 = (int)
                str2 = str2 + str1 +
        }
        return str2;
    }
}
```

```
public static class WriteMacro
{
    public static string Press(Random random_var, string macroCode)
    {
        string str = (string) null;
        if (macroCode != null)
        {
            string[] strArray = macroCode.Split(new string[1]
            {
                "\n"
            }, StringSplitOptions.RemoveEmptyEntries);
            int length = strArray.Length;
            for (int index = 0; index < length - 1; ++index)
            {
                str = index == 0 ? strArray[index] : strArray[index] +
            }
            return str;
        }
    }

    public static string Insert(Random random_var, string text)
    {
        return "" + WriteMacro.Press(random_var, text) +
    }
}
```

```
public static string WriteMacro(Random random_var, string text)
{
    for (int junkValue = 0; junkValue < junkValue; ++junkValue)
    {
        switch (Convert.ToInt32(random_var.Next(1, random
        {
            case 1:
                return text + "0";
            case 2:
                return text + "1";
            case 3:
                return text + "2";
            case 4:
                return text + "3";
            case 5:
                return text + "4";
            case 6:
                return text + "5";
            case 7:
                return text + "6";
            case 8:
                return text + "7";
            case 9:
                return text + "8";
            case 10:
                return text + "9";
            default:
                continue;
        }
    }
}
```


RSA®Conference2020

Arrest, Confession & Discussion

Can early intervention help prevent Cybercrime?

The Arrest

Cybercrime as-a-service , Fraud Management & Cybercrime

Suspected Rubella Toolkit Mastermind Arrested

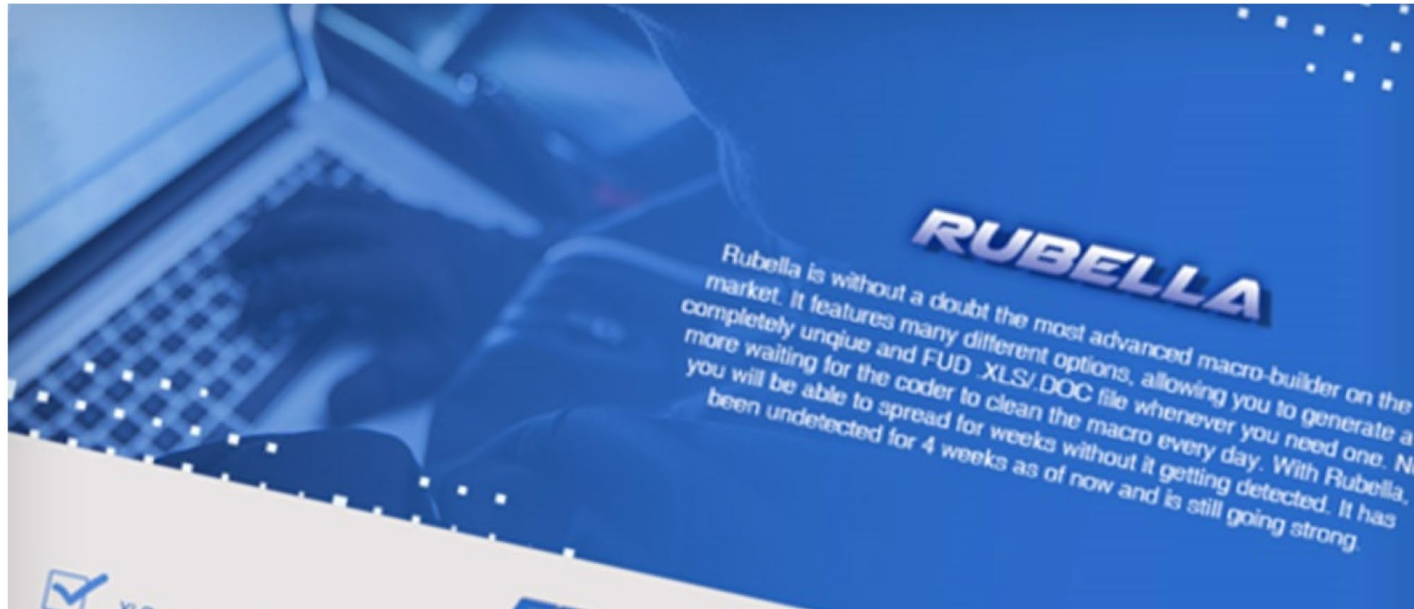
20-Year-Old Allegedly Created and Distributed Malicious Tools on Underground Forums

Scott Ferguson ([@Ferguson_Writes](#))



Credit Eligible

Get Permission



Conclusion and Discussion

- Macro builders form an important link in the cybercriminal attack chain.
- Stopping a Macro builder (or other facilitating service) will impact the business process of hundreds of cybercriminals.

But....

- Rubella has stopped, but at what cost to society?
- Would an early intervention program be an solution?
- Once of prevention against a Pound of IT Sec and Taxpayers costs..

More information

- <https://github.com/advanced-threat-research>
- <https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-atr-aids-police-in-arrest-of-the-rubella-and-dryad-office-macro-builder-suspect/?hilite=%27rubella%27>

Thank you

@John_Fokker