Open Source and Free Tools for Incident Response Teams

Ladislav Bačo

whoami

- Malware and forensics analyst
- Former head of Analytical Department and Department of Cyber Threat Analysis, governmental team CSIRT.SK
- Analyst at Lifars LLC

- https://twitter.com/ladislav_b

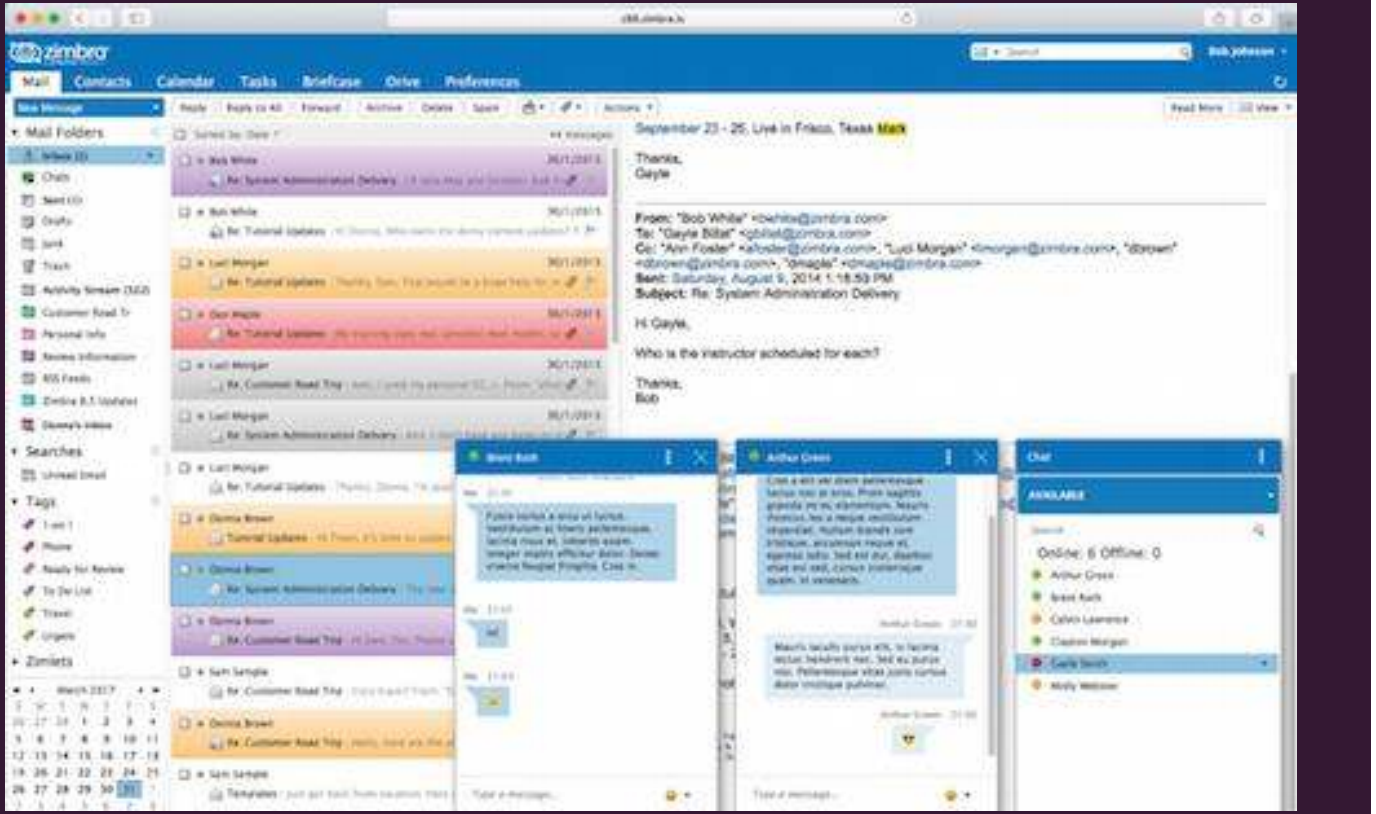
Why?

- Save establishment budget for small CSIRT/CERT
  - Clever and engaged people required
  - Money vs Time

- Overview of (hopefully) useful tools unknown to many people

Team cooperation

- E-Mails, calendars, contacts
  - Postfix, Dovecot
  - Roundcube, RainLoop
  - ThunderBird
  - iRedMail, Zimbra
  - GPG - Kleopatra



September 23 - 25, Live in Frisco, Texas Mark

Thanks,
Gayle

From: "Bob White" <bwhite@zimbra.com>
To: "Gayle Billat" <gbillat@zimbra.com>
Cc: "Ann Foster" <afoster@zimbra.com>, "Luci Morgan" <lmorgan@zimbra.com>, "dbrown" <dbrown@zimbra.com>, "dmaple" <dmaple@zimbra.com>
Sent: Saturday, August 9, 2014 1:18:53 PM
Subject: Re: System Administration Delivery

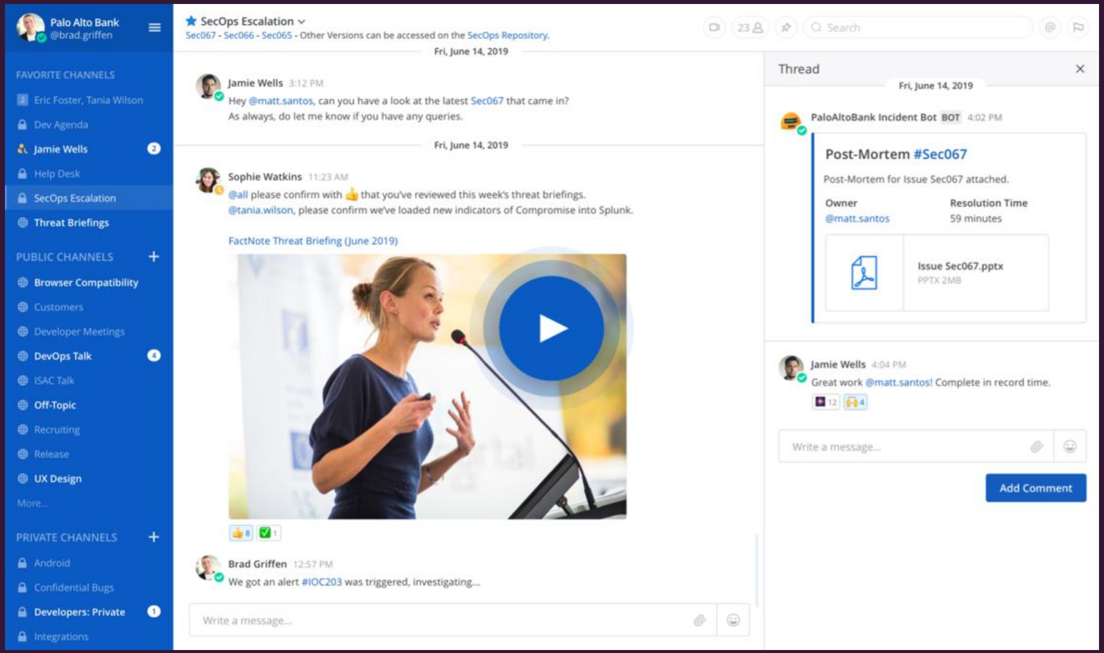
Hi Gayle,

Who is the instructor scheduled for each?

Thanks,
Bob

Team cooperation

- Team chat
  - Rocket.chat
  - Mattermost



SecOps Escalation

Sec067 - Sec066 - Sec065 - Other Versions can be accessed on the SecOps Repository.

Fri, June 14, 2019

Jamie Wells 3:12 PM
Hey @matt.santos, can you have a look at the latest Sec067 that came in?
As always, do let me know if you have any queries.

Fri, June 14, 2019

Sophie Watkins 11:23 AM
@all please confirm with 👍 that you've reviewed this week's threat briefings.
@tania.wilson, please confirm we've loaded new indicators of Compromise into Splunk.

FactNote Threat Briefing (June 2019)

👍 8 ✅ 1

Brad Griffen 12:57 PM
We got an alert #IOC203 was triggered, investigating...

Fri, June 14, 2019

PaloAltoBank Incident Bot BOT 4:02 PM

Post-Mortem #Sec067

Post-Mortem for Issue Sec067 attached.

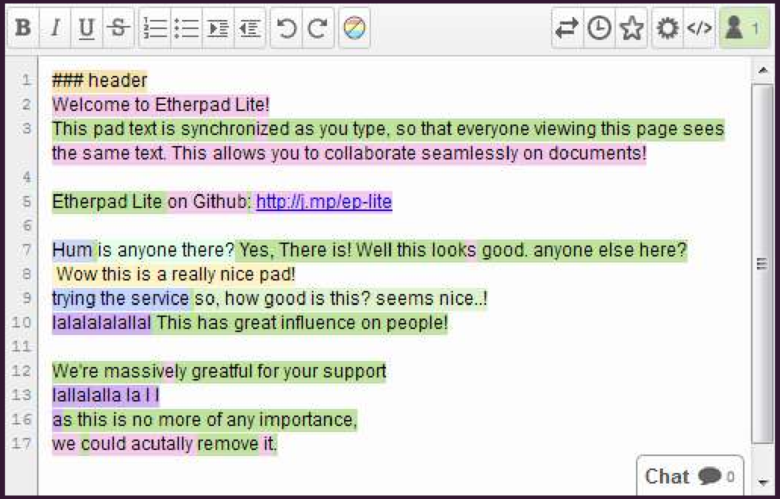
Owner	Resolution Time
@matt.santos	59 minutes

Issue Sec067.pptx
PPTX 2MB

Jamie Wells 4:04 PM
Great work @matt.santos! Complete in record time.

12 🙌 4

- Collaborative documents (notepads)
  - Etherpad
- Wiki & Docs
  - MediaWiki, DokuWiki
  - MkDocs



header
Welcome to Etherpad Lite!
This pad text is synchronized as you type, so that everyone viewing this page sees the same text. This allows you to collaborate seamlessly on documents!

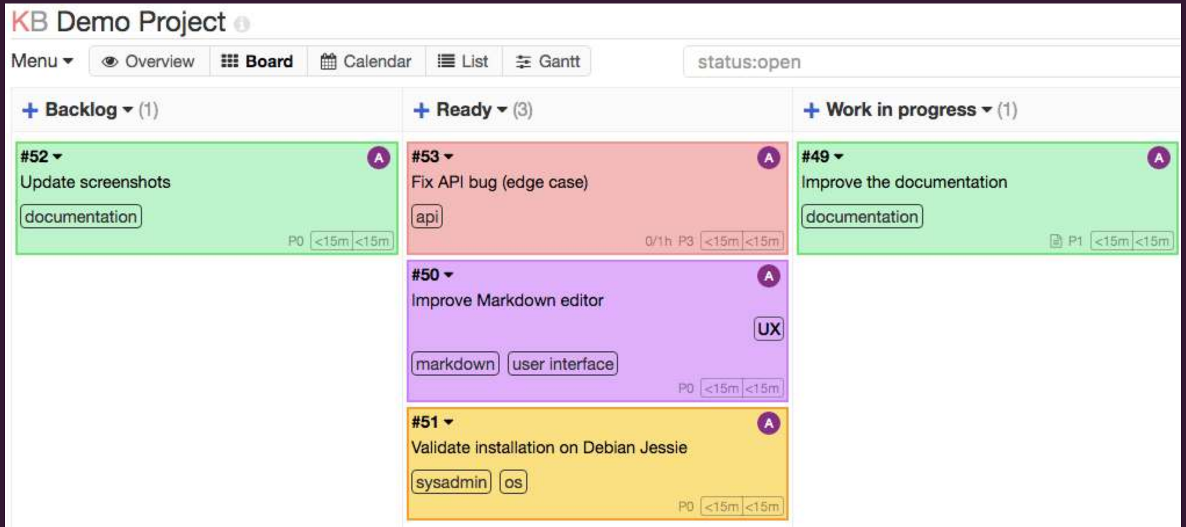
Etherpad Lite on Github: http://j.mp/ep-lite

Hum is anyone there? Yes, There is! Well this looks good. anyone else here?
 Wow this is a really nice pad!
trying the service so, how good is this? seems nice..!
lalalalalalal This has great influence on people!

We're massively greatful for your support
lallalalla la l l
as this is no more of any importance,
we could acutally remove it.

Team cooperation

- Project and task management
  - OpenProject
  - Wekan
  - Kanboard



#52
Update screenshots
documentation
P0 <15m <15m

#53
Fix API bug (edge case)
api
0/1h P3 <15m <15m

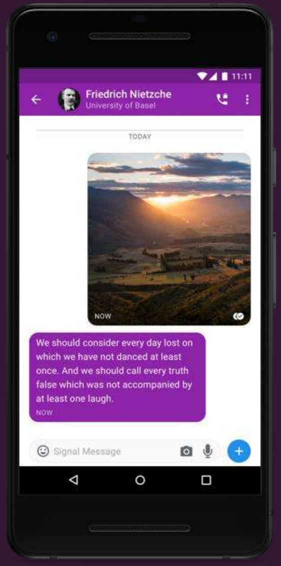
#50
Improve Markdown editor
UX
markdown user interface
P0 <15m <15m

#51
Validate installation on Debian Jessie
sysadmin os
P0 <15m <15m

#49
Improve the documentation
documentation
P1 <15m <15m

Team cooperation

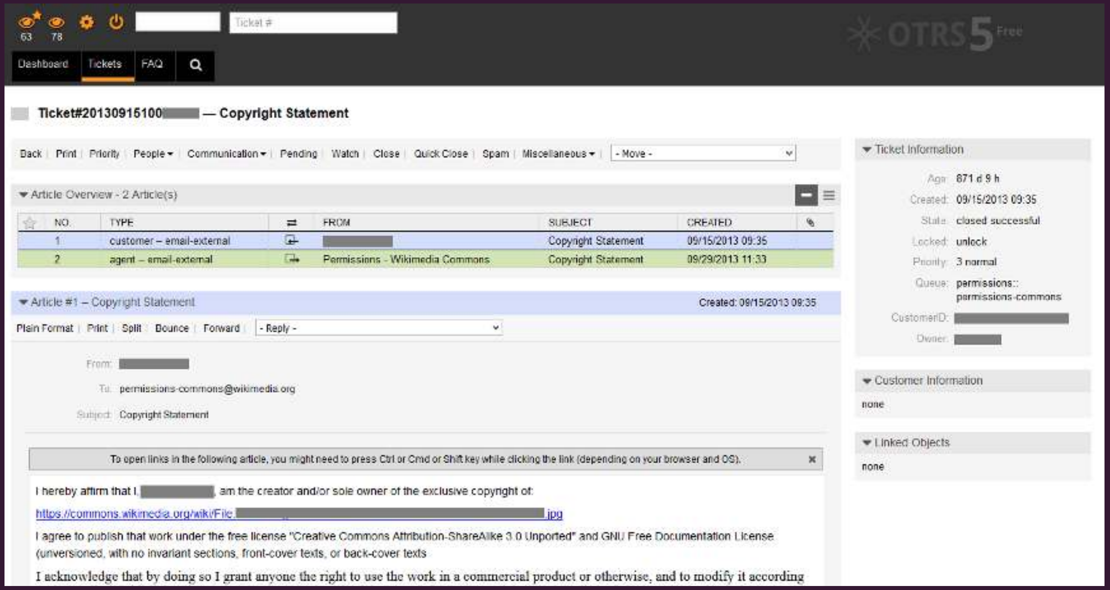
- Secure access - 2FA
  - Certificates – only authorized persons can access the interface
- Secure messaging, (group)calls, video, screen sharing
  - Signal, Telegram, Wire... but no one-fits-all



We should consider every day lost on which we have not danced at least once. And we should call every truth false which was not accompanied by at least one laugh.

Incident handling, response, infoshare

- Ticketing system – mails, calls, notes, customers, stats,…
  - RTIR, OTRS
  - Redmine


63
78
Ticket #
OTRS 5 Free
Dashboard
Tickets
FAQ
Back | Print | Priority | People ▾ | Communication ▾ | Pending | Watch | Close | Quick Close | Spam | Miscellaneous ▾ | - Move -
Plain Format | Print | Split | Bounce | Forward | - Reply -

Ticket#20130915100[redacted] — Copyright Statement

Article Overview - 2 Article(s)

NO.	TYPE	FROM	SUBJECT	CREATED
1	customer – email-external	[redacted]	Copyright Statement	09/15/2013 09:35
2	agent – email-external	Permissions - Wikimedia Commons	Copyright Statement	09/29/2013 11:33

Article #1 – Copyright Statement — Created: 09/15/2013 09:35

From: [redacted]
To: permissions-commons@wikimedia.org
Subject: Copyright Statement

To open links in the following article, you might need to press Ctrl or Cmd or Shift key while clicking the link (depending on your browser and OS).

I hereby affirm that I, [redacted], am the creator and/or sole owner of the exclusive copyright of:

https://commons.wikimedia.org/wiki/File:[redacted].jpg

I agree to publish that work under the free license "Creative Commons Attribution-ShareAlike 3.0 Unported" and GNU Free Documentation License (unversioned, with no invariant sections, front-cover texts, or back-cover texts

I acknowledge that by doing so I grant anyone the right to use the work in a commercial product or otherwise, and to modify it according

Ticket Information

Age: 871 d 9 h
Created: 09/15/2013 09:35
State: closed successful
Locked: unlock
Priority: 3 normal
Queue: permissions::permissions-commons
CustomerID: [redacted]
Owner: [redacted]

Customer Information

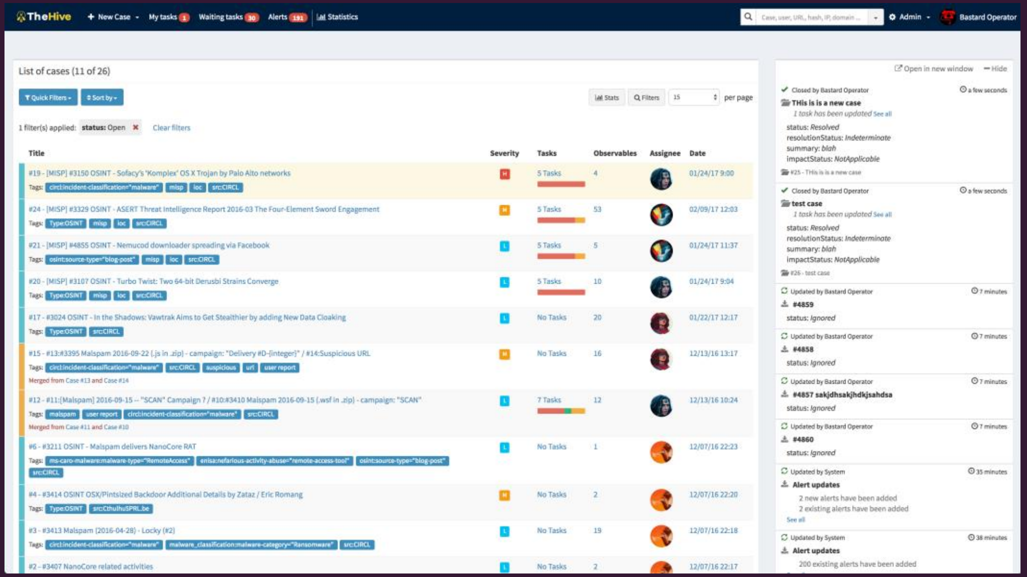
none

Linked Objects

none

Incident handling, response, infoshare

- TheHive Project
- Demisto Free Community Edition



List of cases (11 of 26)

1 filter(s) applied: **status:** Open ✕ Clear filters

Title	Severity	Tasks	Observables	Assignee	Date
#19 - [MISP] #3150 OSINT - Sofacy's 'Komplex' OS X Trojan by Palo Alto networks Tags: circl:incident-classification="malware" misp ioc src:CIRCL	H	5 Tasks	4		01/24/17 9:00
#24 - [MISP] #3329 OSINT - ASERT Threat Intelligence Report 2016-03 The Four-Element Sword Engagement Tags: Type:OSINT misp ioc src:CIRCL	M	5 Tasks	53		02/09/17 12:03
#21 - [MISP] #4855 OSINT - Nemucod downloader spreading via Facebook Tags: osint:source-type="blog-post" misp ioc src:CIRCL	L	5 Tasks	5		01/24/17 11:37
#20 - [MISP] #3107 OSINT - Turbo Twist: Two 64-bit Derusbi Strains Converge Tags: Type:OSINT misp ioc src:CIRCL	L	5 Tasks	10		01/24/17 9:04
#17 - #3024 OSINT - In the Shadows: Vawtrak Aims to Get Stealthier by adding New Data Cloaking Tags: Type:OSINT src:CIRCL	L	No Tasks	20		01/22/17 12:17
#15 - #13:#3395 Malspam 2016-09-22 (.js in .zip) - campaign: "Delivery #D-[integer]" / #14:Suspicious URL Tags: circl:incident-classification="malware" src:CIRCL suspicious url user report Merged from Case #13 and Case #14	M	No Tasks	16		12/13/16 13:17
#12 - #11:[Malspam] 2016-09-15 -- "SCAN" Campaign ? / #10:#3410 Malspam 2016-09-15 (.wsf in .zip) - campaign: "SCAN" Tags: malspam user report circl:incident-classification="malware" src:CIRCL Merged from Case #11 and Case #10	L	7 Tasks	12		12/13/16 10:24
#6 - #3211 OSINT - Malspam delivers NanoCore RAT Tags: ms-caro-malware:malware-type="RemoteAccess" enisa:nefarious-activity-abuse="remote-access-tool" osint:source-type="blog-post" src:CIRCL	L	No Tasks	1		12/07/16 22:23
#4 - #3414 OSINT OSX/Pintsized Backdoor Additional Details by Zataz / Eric Romang Tags: Type:OSINT src:CthulhuSPRL.be	M	No Tasks	2		12/07/16 22:20
#3 - #3413 Malspam (2016-04-28) - Locky (#2) Tags: circl:incident-classification="malware" malware_classification:malware-category="Ransomware" src:CIRCL	L	No Tasks	19		12/07/16 22:18
#2 - #3407 NanoCore related activities	L	No Tasks	2		12/07/16 22:17

Closed by Bastard Operator — a few seconds
THis is is a new case
1 task has been updated See all
status: *Resolved*
resolutionStatus: *Indeterminate*
summary: *blah*
impactStatus: *NotApplicable*
#25 - THis is is a new case

Closed by Bastard Operator — a few seconds
test case
1 task has been updated See all
status: *Resolved*
resolutionStatus: *Indeterminate*
summary: *blah*
impactStatus: *NotApplicable*
#26 - test case

Updated by Bastard Operator — 7 minutes
#4859
status: *Ignored*

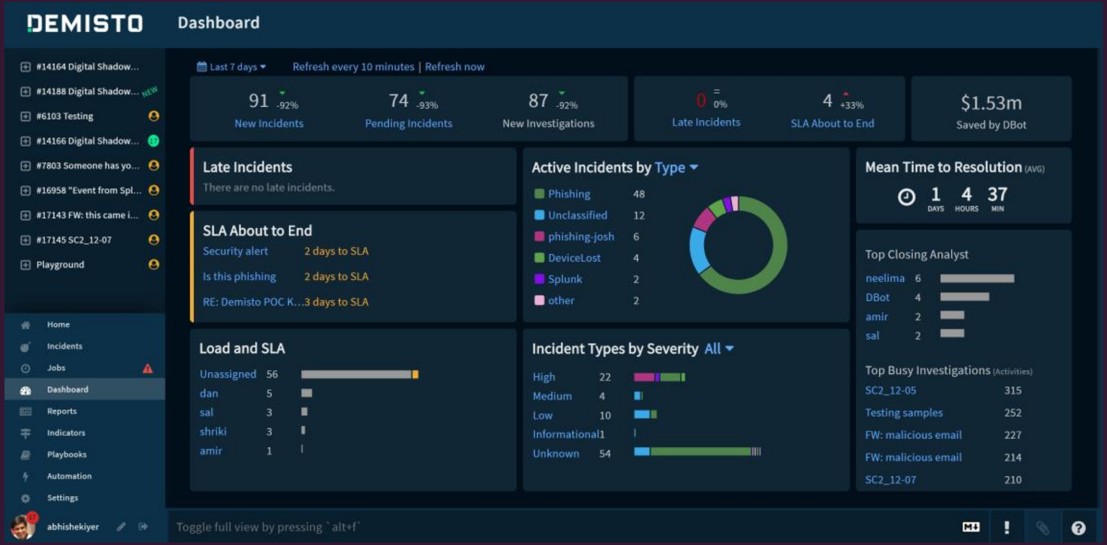
Updated by Bastard Operator — 7 minutes
#4858
status: *Ignored*

Updated by Bastard Operator — 7 minutes
#4857 sakjdhsakjhdkjsahdsa
status: *Ignored*

Updated by Bastard Operator — 7 minutes
#4860
status: *Ignored*

Updated by System — 35 minutes
Alert updates
2 new alerts have been added
2 existing alerts have been added
See all

Updated by System — 38 minutes
Alert updates
200 existing alerts have been added



#14164 Digital Shadow...
#14188 Digital Shadow...
#6103 Testing
#14166 Digital Shadow...
#7803 Someone has yo...
#16958 "Event from Spl...
#17143 FW: this came i...
#17145 SC2_12-07
Playground

91 -92% New Incidents
74 -93% Pending Incidents
87 -92% New Investigations
0 = 0% Late Incidents
4 +33% SLA About to End
$1.53m Saved by DBot

Late Incidents
There are no late incidents.

SLA About to End

Security alert	2 days to SLA
Is this phishing	2 days to SLA
RE: Demisto POC K...	3 days to SLA

Active Incidents by Type

Phishing	48
Unclassified	12
phishing-josh	6
DeviceLost	4
Splunk	2
other	2

Mean Time to Resolution (AVG)
1 DAYS 4 HOURS 37 MIN

Load and SLA

Unassigned	56
dan	5
sal	3
shriki	3
amir	1

Incident Types by Severity All

High	22
Medium	4
Low	10
Informational	1
Unknown	54

Top Closing Analyst

neelima	6
DBot	4
amir	2
sal	2

Top Busy Investigations (Activities)

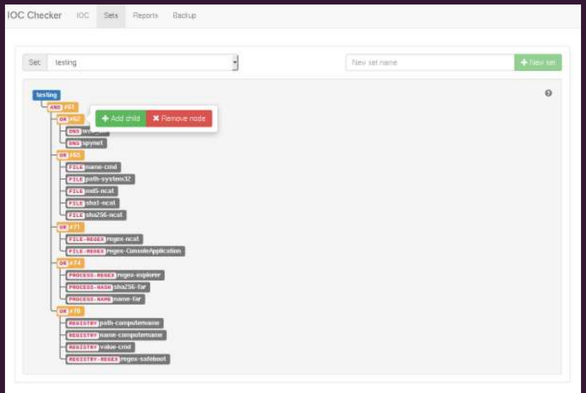
SC2_12-05	315
Testing samples	252
FW: malicious email	227
FW: malicious email	214
SC2_12-07	210

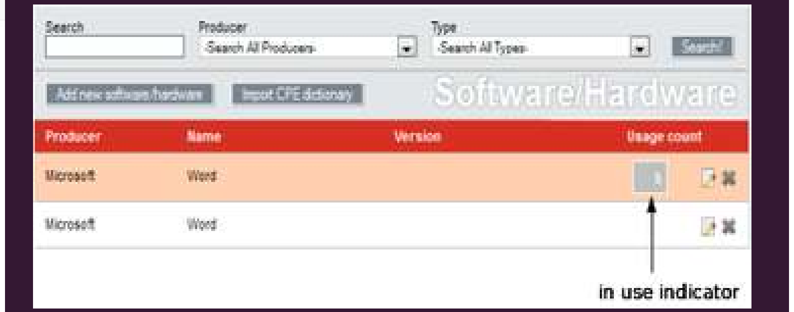
Toggle full view by pressing `alt+f`

Incident handling, response, infoshare

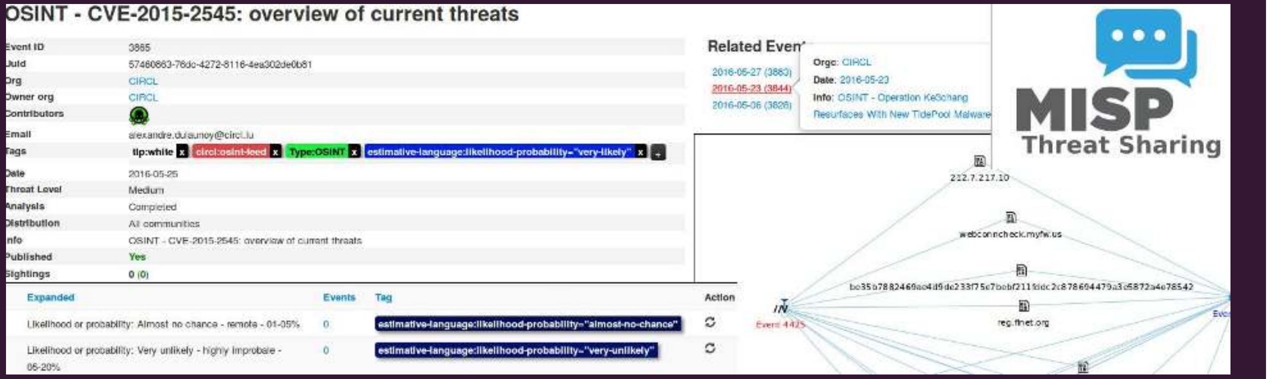
- Vulnerability, news, advisories
  - Taranis3
- IoC sharing
  - MISP
- IoC checker by CSIRT.SK

- Integrations
- **Automatization!**





Producer	Name	Version	Usage count
Microsoft	Word		
Microsoft	Word		



OSINT - CVE-2015-2545: overview of current threats

Event ID	3865
Uuid	57460863-76dc-4272-8116-4ea302de0b81
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tlp:white x circl:osint-feed x Type:OSINT x estimative-language:likelihood-probability="very-likely" x +
Date	2016-05-25
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	OSINT - CVE-2015-2545: overview of current threats
Published	Yes
Sightings	0 (0)

Related Event

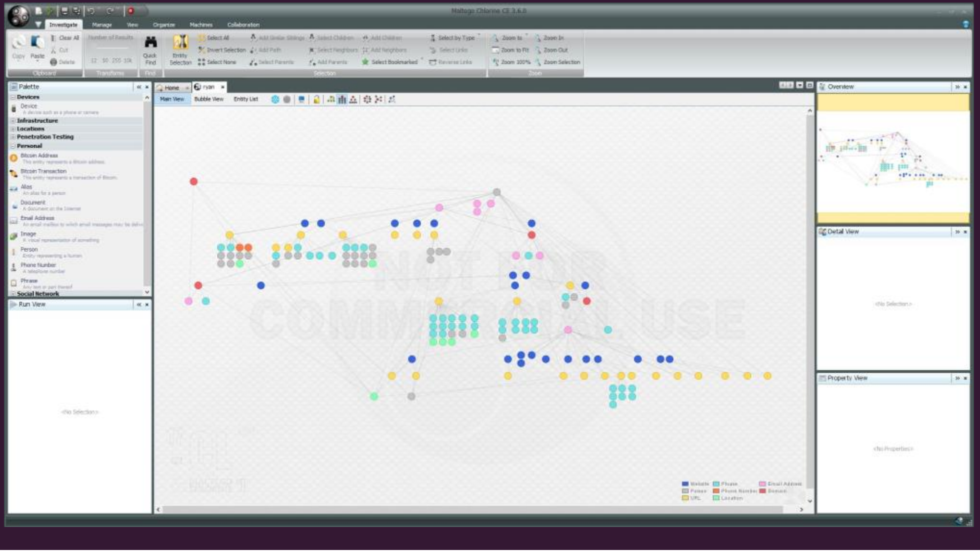
2016-05-27 (3883)
2016-05-23 (3844)
2016-05-06 (3826)

Orgc: CIRCL
Date: 2016-05-23
Info: OSINT - Operation KeSchang Resurfaces With New TidePool Malware

Expanded	Events	Tag	Action
Likelihood or probability: Almost no chance - remote - 01-05%	0	estimative-language:likelihood-probability="almost-no-chance"	
Likelihood or probability: Very unlikely - highly improbable - 05-20%	0	estimative-language:likelihood-probability="very-unlikely"	

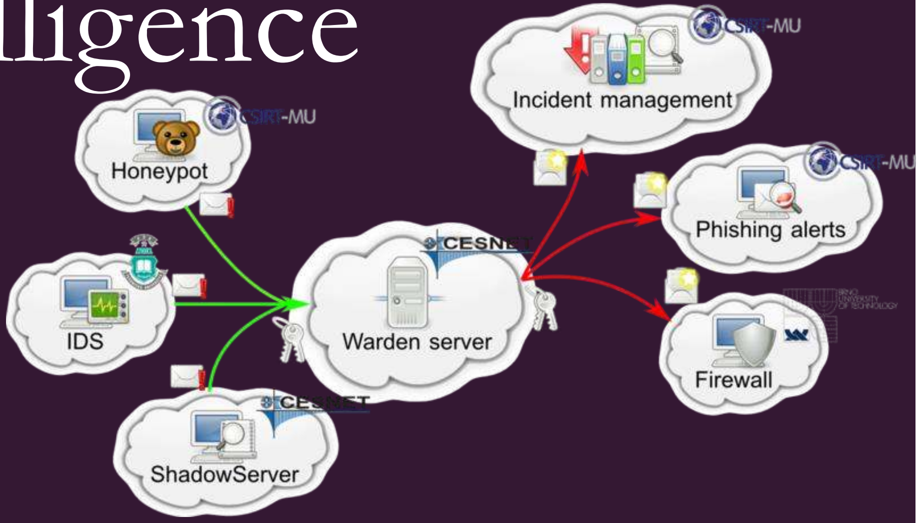
OSInt, Recon, Threat Intelligence

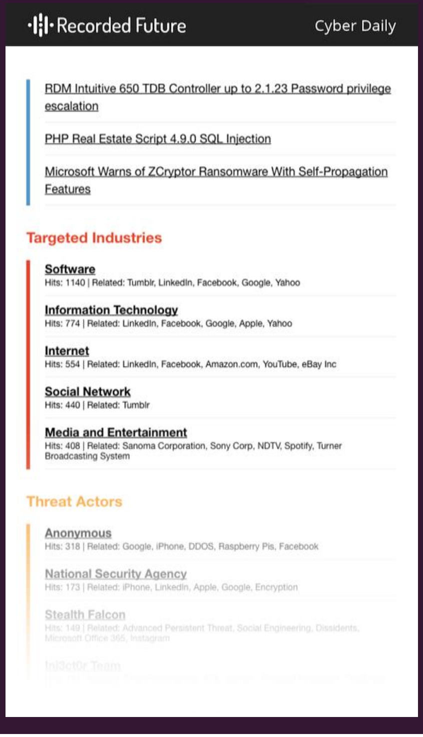
- OpenSource Intelligence and Recon
  - GeoIP, WhoIS, passive dns
  - VirusTotal, Google Safe Browsing, urlscan.io, urlhaus
  - Google Dorks (GHDB)
  - Shodan, Censys, (nmap)
  - Maltego CE
  - *TorBrowser, VPNs, Proxies*



OSInt, Recon, Threat Intelligence

- Feeds collecting and processing
  - IntelMQ, Warden
- Threat Intelligence
  - RiskIQ, OpenCTI
  - ThreatMiner, ThreatConnect
  - *??Relevant Feeds??*
  - RecordedFuture CyberDaily





Recorded Future Cyber Daily

RDM Intuitive 650 TDB Controller up to 2.1.23 Password privilege escalation

PHP Real Estate Script 4.9.0 SQL Injection

Microsoft Warns of ZCryptor Ransomware With Self-Propagation Features

Targeted Industries

Software
Hits: 1140 | Related: Tumblr, LinkedIn, Facebook, Google, Yahoo

Information Technology
Hits: 774 | Related: LinkedIn, Facebook, Google, Apple, Yahoo

Internet
Hits: 554 | Related: LinkedIn, Facebook, Amazon.com, YouTube, eBay Inc

Social Network
Hits: 440 | Related: Tumblr

Media and Entertainment
Hits: 408 | Related: Sanoma Corporation, Sony Corp, NDTV, Spotify, Turner Broadcasting System

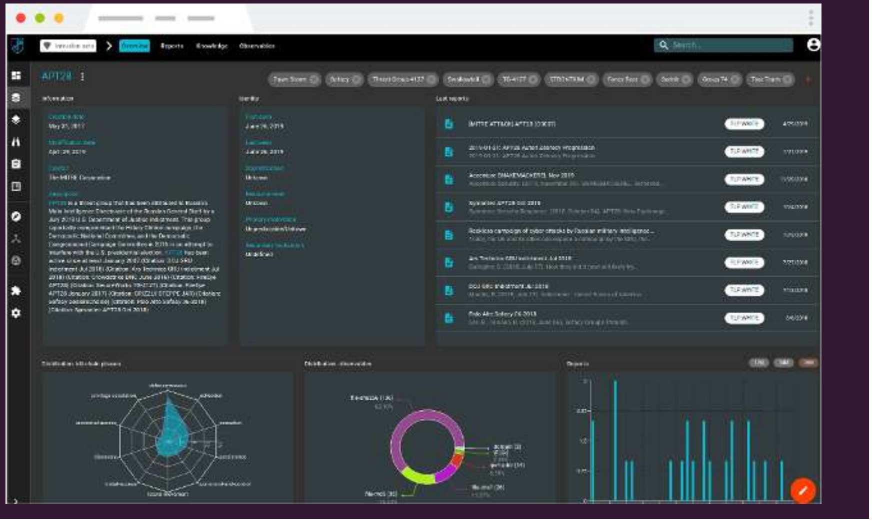
Threat Actors

Anonymous
Hits: 318 | Related: Google, iPhone, DDOS, Raspberry Pis, Facebook

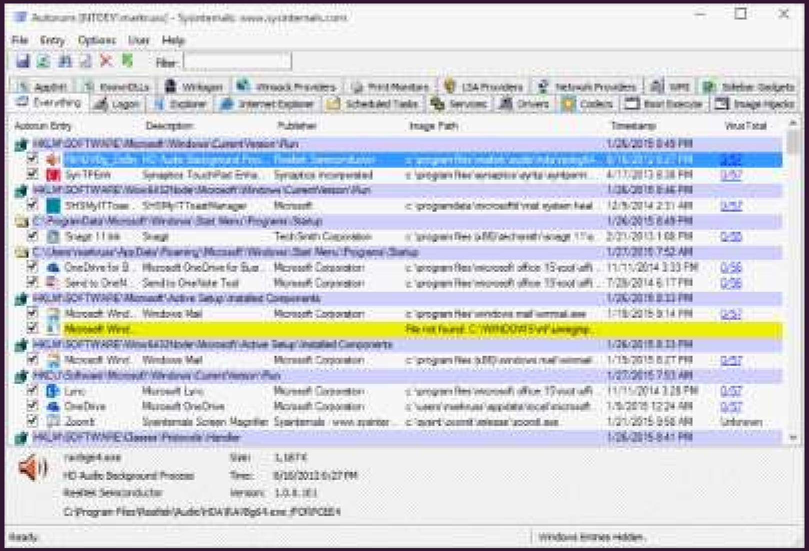
National Security Agency
Hits: 173 | Related: iPhone, LinkedIn, Apple, Google, Encryption

Stealth Falcon
Hits: 149 | Related: Advanced Persistent Threat, Social Engineering, Dissidents, Microsoft Office 365, Instagram

Inj3ct0r Team



Forensics

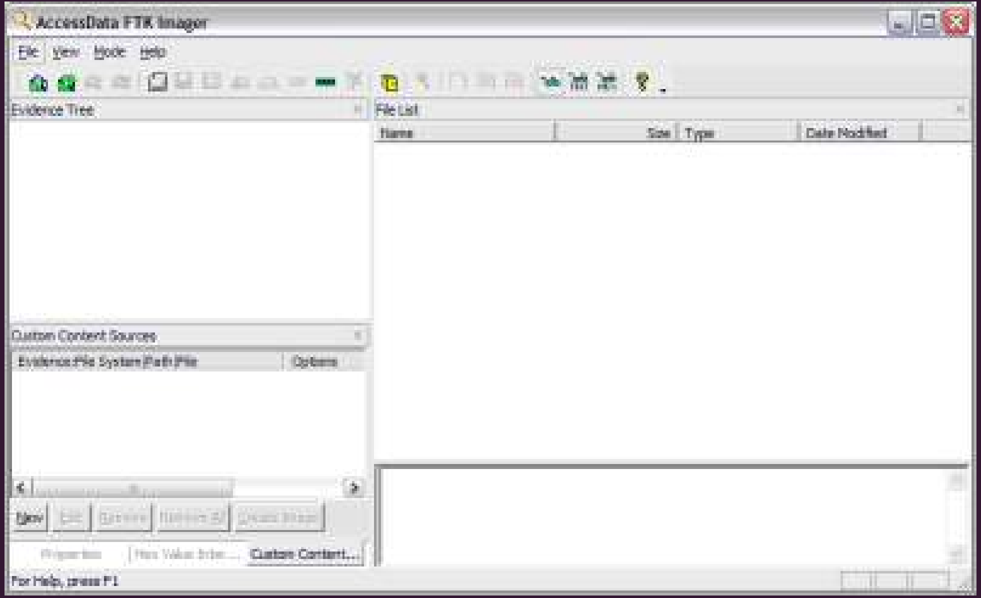


Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				1/26/2015 8:45 PM	
☑ RtHDVBg_Dolby	HD Audio Background Pro...	Realtek Semiconductor	c:\program files\realtek\audio\hda\ravbg64...	8/16/2012 6:27 PM	0/57
☑ SynTPEnh	Synaptics TouchPad Enha...	Synaptics Incorporated	c:\program files\synaptics\syntp\syntpenh...	4/17/2013 8:38 PM	0/57
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				1/26/2015 8:46 PM	
☑ SHSMyITTicon...	SHSMyITTaskManager	Microsoft	c:\programdata\microsoft\vmsl system heal...	12/9/2014 2:31 AM	0/57
C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup				1/26/2015 8:49 PM	
☑ Snagit 11.lnk	Snagit	TechSmith Corporation	c:\program files (x86)\techsmith\snagit 11\s...	2/21/2013 1:08 PM	0/55
C:\Users\markruss\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				1/27/2015 7:52 AM	
☑ OneDrive for B...	Microsoft OneDrive for Bus...	Microsoft Corporation	c:\program files\microsoft office 15\root\vfs...	11/11/2014 3:33 PM	0/56
☑ Send to OneN...	Send to OneNote Tool	Microsoft Corporation	c:\program files\microsoft office 15\root\vfs...	7/28/2014 6:17 PM	0/56
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				1/26/2015 8:33 PM	
☑ Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files\windows mail\winmail.exe	1/15/2015 8:14 PM	0/57
☑ Microsoft Wind...			File not found: C:\WINDOWS\inf\unregmp...		
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				1/26/2015 8:33 PM	
☑ Microsoft Wind...	Windows Mail	Microsoft Corporation	c:\program files (x86)\windows mail\winmail...	1/15/2015 8:27 PM	0/57
HKCU\Software\Microsoft\Windows\CurrentVersion\Run				1/27/2015 7:53 AM	
☑ Lync	Microsoft Lync	Microsoft Corporation	c:\program files\microsoft office 15\root\vfs...	11/11/2014 3:28 PM	0/57
☑ OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\markruss\appdata\local\microsoft...	1/9/2015 12:24 AM	0/57
☑ ZoomIt	Sysinternals Screen Magnifier	Sysinternals - www.sysinter...	c:\zoomit\zoomit\release\zoomit.exe	1/21/2015 9:56 AM	Unknown
HKLM\SOFTWARE\Classes\Protocols\Handler				1/26/2015 8:41 PM	

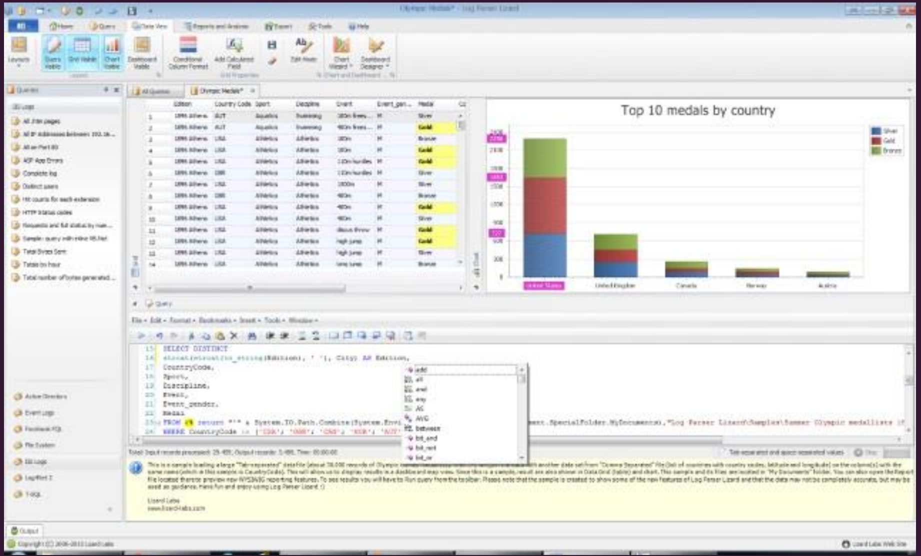
ravbg64.exe Size: 1,187 K
HD Audio Background Process Time: 8/16/2012 6:27 PM
Realtek Semiconductor Version: 1.0.6.161
C:\Program Files\Realtek\Audio\HDA\RAVBg64.exe /FORPCEE4

Ready. | Windows Entries Hidden.

- Live Forensics and Incident Response
  - SysInternals Suite (ProcExp, Autoruns, Sysmon), Nirsoft utilities
  - debsums
- Image acquisition and mounting
  - dcfldd, dc3dd, FTK Imager Lite
  - Affuse, winregfs



Forensics

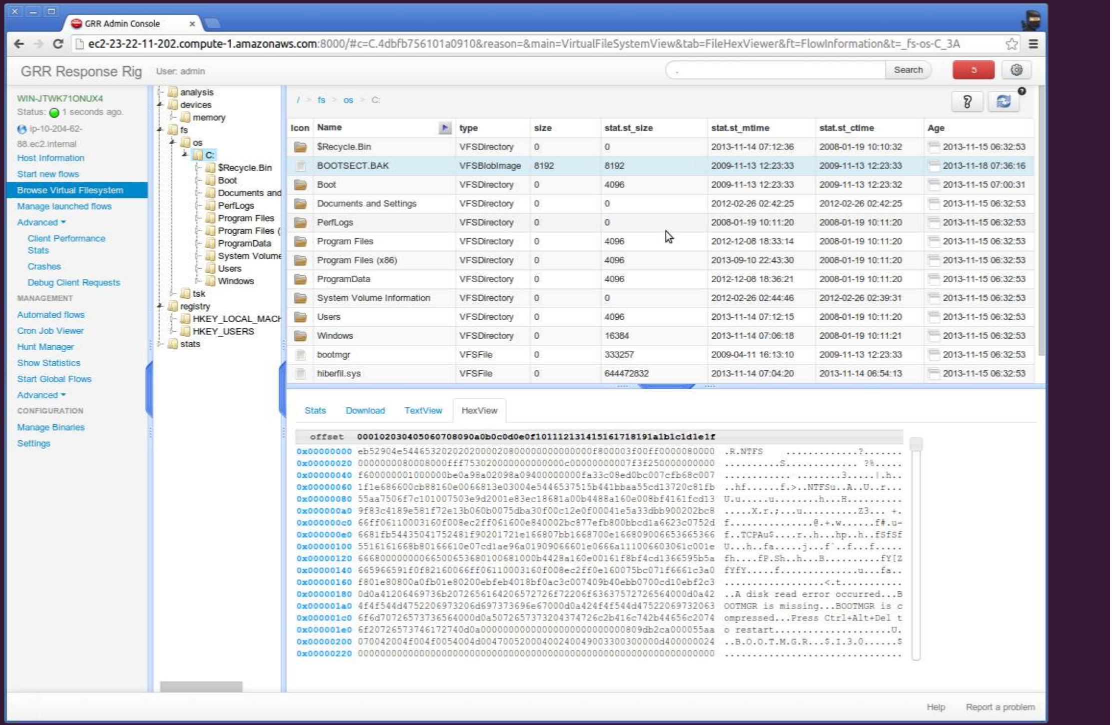


```
SELECT DISTINCT
CountryCode,
Sport,
Discipline,
Event,
Event_gender,
Medal
```

- Log and filesystem processing
  - Photorec, recuva, diskdigger, scalpel
  - Lynis, ClamAV (and others AVs), chkrootkit, rkhunter
  - Log2Timeline + grep, sed, awk, perl, python + LibreOffice Calc (or Excel)
  - Log Parser Lizard
  - (autopsy), apache-scalp, ELK (Elastic+LogStash+Kibana)

Forensics

- Memory acquisition
  - FTK Imager Lite, winpmem, LIME
- Memory analysis
  - Rekall, volatility
    - *profiles*
- Endpoint analysis
  - Google Rapid Response (Rekall included)



Icon	Name	type	size	stat.st_size	stat.st_mtime	stat.st_ctime	Age
	$Recycle.Bin	VFSDirectory	0	0	2013-11-14 07:12:36	2008-01-19 10:10:32	2013-11-15 06:32:53
	BOOTSECT.BAK	VFSBlobImage	8192	8192	2009-11-13 12:23:33	2009-11-13 12:23:33	2013-11-18 07:36:16
	Boot	VFSDirectory	0	4096	2009-11-13 12:23:33	2009-11-13 12:23:32	2013-11-15 07:00:31
	Documents and Settings	VFSDirectory	0	0	2012-02-26 02:42:25	2012-02-26 02:42:25	2013-11-15 06:32:53
	PerfLogs	VFSDirectory	0	0	2008-01-19 10:11:20	2008-01-19 10:11:20	2013-11-15 06:32:53
	Program Files	VFSDirectory	0	4096	2012-12-08 18:33:14	2008-01-19 10:11:20	2013-11-15 06:32:53
	Program Files (x86)	VFSDirectory	0	4096	2013-09-10 22:43:30	2008-01-19 10:11:20	2013-11-15 06:32:53
	ProgramData	VFSDirectory	0	4096	2012-12-08 18:36:21	2008-01-19 10:11:20	2013-11-15 06:32:53
	System Volume Information	VFSDirectory	0	0	2012-02-26 02:44:46	2012-02-26 02:39:31	2013-11-15 06:32:53
	Users	VFSDirectory	0	4096	2013-11-14 07:12:15	2008-01-19 10:11:20	2013-11-15 06:32:53
	Windows	VFSDirectory	0	16384	2013-11-14 07:06:18	2008-01-19 10:11:21	2013-11-15 06:32:53
	bootmgr	VFSFile	0	333257	2009-04-11 16:13:10	2009-11-13 12:23:33	2013-11-15 06:32:53
	hiberfil.sys	VFSFile	0	644472832	2013-11-14 07:04:20	2013-11-14 06:54:13	2013-11-15 06:32:53

```
  offset   000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f
0x00000000 eb52904e5446532020202000020800000000000000f800003f00ff0000080000 .R.NTFS    .............?.......
0x00000020 00000000800080000fff7530200000000000000c0000000007f3f250000000000 ..........S............ ?%.....
0x00000040 f6000000010000000be0a98a02098a09400000000fa33c08ed0bc007cfb68c007 ............ ........3.....|.h..
0x00000060 1f1e686600cb88160e0066813e03004e5446537515b441bbaa55cd13720c81fb ..hf......f.>..NTFSu..A..U..r...
0x00000080 55aa7506f7c101007503e9d2001e83ec18681a00b4488a160e008bf4161fcd13 U.u.....u........h...H..........
0x000000a0 9f83c4189e581f72e13b060b0075dba30f00c12e0f00041e5a33dbb900202bc8 .....X.r.;...u..........Z3... +.
0x000000c0 66ff06110003160f008ec2ff061600e840002bc877efb800bbcd1a6623c0752d f...............@.+.w......f#.u-
0x000000e0 6681fb54435041752481f90201721e166807bb1668700e16680900665366536 6 f..TCPAu$....r..h...hp..h..fSfSf
0x00000100 5516161668b80166610e07cd1ae96a01909066601e0666a111006603061c001e U...h..fa.....j...f`..f...f.....
0x00000120 6668000000006650065368010068100b4428a160e00161f8bf4cd1366595b5a fh.....fP.Sh..h...B..........fY[Z
0x00000140 665966591f0f82160066ff06110003160f008ec2ff0e160075bc071f6661c3a0 fYfY.....f..............u...fa..
0x00000160 f801e80800a0fb01e80200ebfeb4018bf0ac3c007409b40ebb0700cd10ebf2c3 ..................<.t...........
0x00000180 0d0a41206469736b2072656164206572726f72206f63637572726564000d0a42 ..A disk read error occurred...B
0x000001a0 4f4f544d4752206973206d697373696e67000d0a424f4f544d47522069732063 OOTMGR is missing...BOOTMGR is c
0x000001c0 6f6d7072657373656400d0a507265737320437472c2b416c742b44656c2074 ompressed...Press Ctrl+Alt+Del t
0x000001e0 6f207265737461727400d0a0000000000000000000000000809db2ca000055aa o restart...................U.
0x00000200 070042004f004f0054004d00470052000400240049003300300000d400000024 ..B.O.O.T.M.G.R...$.I.3.0......$
0x00000220 0000000000000000000000000000000000000000000000000000000000000000 ................................
```

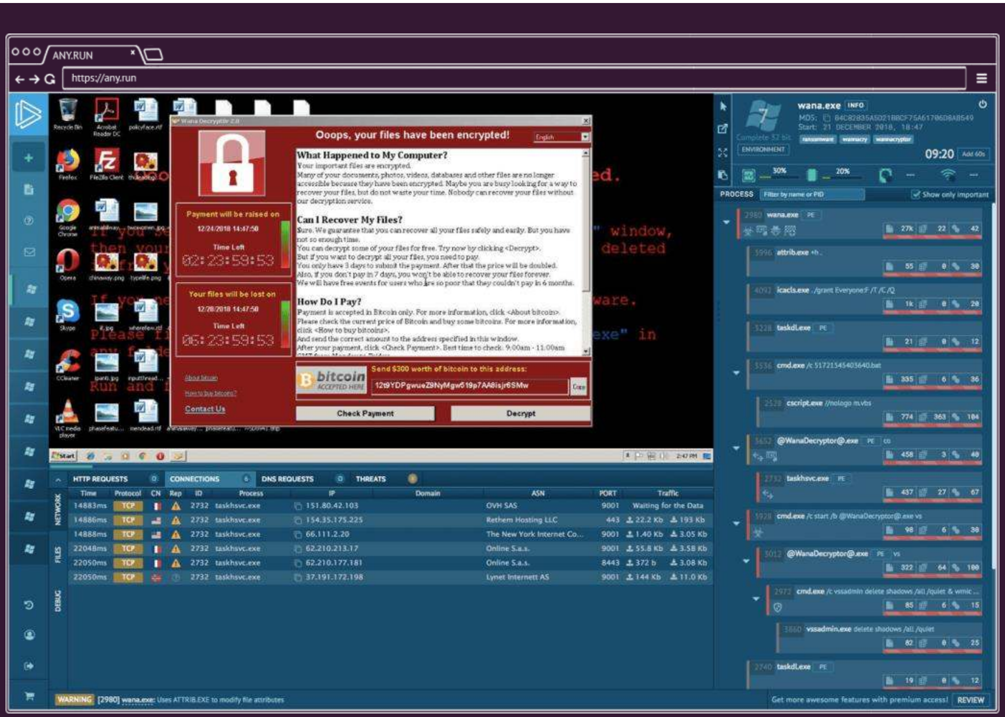
Forensics

- Linux distributions
  - CAINE Live
  - Kali
  - SIFT Workstation

QuickTime Player File Edit View Window Help
Ubuntu Desktop
mount_points
Network-Forensics-Poster.pdf
cases
Rekall-Cheatsheet.pdf
DFIR-Smartphone-Forensics-Poster.pdf
SIFT-Cheatsheet.pdf
DFIR-Threat-Intel-Poster.pdf
SIFT-REMnux-Poster.pdf
Find-Evil.pdf
Volatility-Cheatsheet.pdf
Hex-File-Regex-Cheatsheet.pdf
Windows-Forensics-Poster.pdf
Linux-Shell-Survival-Guide.pdf
Windows-to-Unix-Cheatsheet.pdf
Memory-Forensics-Poster.pdf
SIFT
WORKSTATION

Malware Analysis

- Online services
  - Repos and DB
    - VirusTotal, VirusShare
  - Sandboxes
    - Hybrid-analysis, Any.Run
  - Classification
    - Intezer, NoDistribute



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
12/24/2018 14:47:50
Time Left
02:23:59:53

Your files will be lost on
12/28/2018 14:47:50
Time Left
06:23:59:53

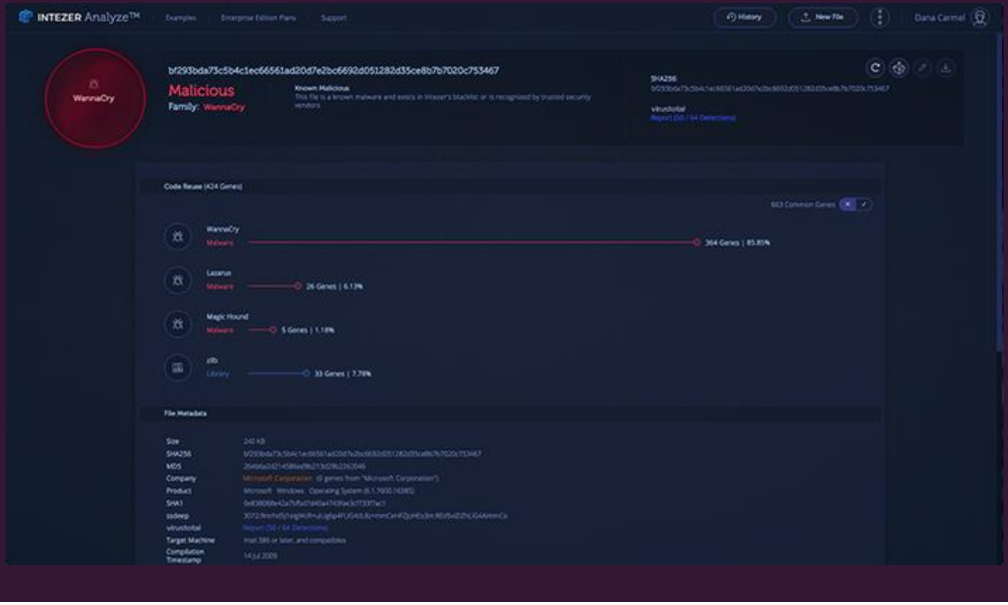
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Check Payment | Decrypt

Time	Protocol	CN	Rep	ID	Process	IP	Domain	ASN	PORT	Traffic
14883ms	TCP		⚠	2732	taskhsvc.exe	151.80.42.103		OVH SAS	9001	Waiting for the Data
14886ms	TCP		⚠	2732	taskhsvc.exe	154.35.175.225		Rethem Hosting LLC	443	22.2 Kb 193 Kb
14888ms	TCP		⚠	2732	taskhsvc.exe	66.111.2.20		The New York Internet Co...	9001	1.40 Kb 3.05 Kb
22048ms	TCP		⚠	2732	taskhsvc.exe	62.210.213.17		Online S.a.s.	9001	55.8 Kb 3.58 Kb
22050ms	TCP		⚠	2732	taskhsvc.exe	62.210.177.181		Online S.a.s.	8443	372 b 3.08 Kb
22050ms	TCP			2732	taskhsvc.exe	37.191.172.198		Lynet Internett AS	9001	144 Kb 11.0 Kb

WARNING [2980] wana.exe: Uses ATTRIB.EXE to modify file attributes

Get more awesome features with premium access! REVIEW



bf293bda73c5b4c1ec66561ad20d7e2bc6692d051282d35ce8b7b7020c753467

Malicious
Family: WannaCry

Known Malicious
This file is a known malware and exists in Intezer's blacklist or is recognized by trusted security vendors

Code Reuse (424 Genes)

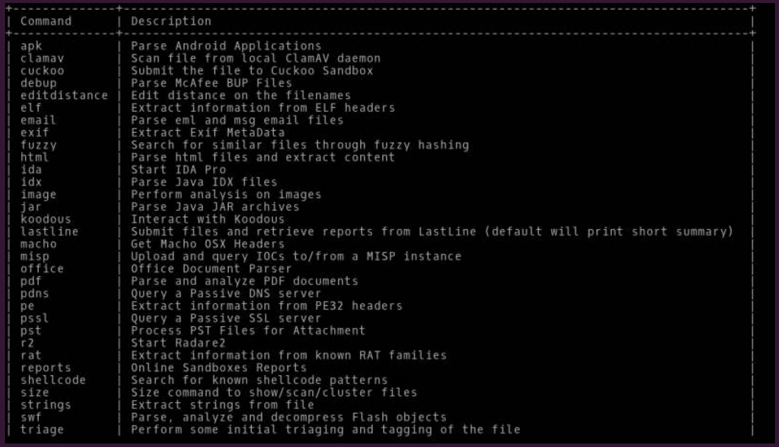
WannaCry	Malware	364 Genes | 85.85%
Lazarus	Malware	26 Genes | 6.13%
Magic Hound	Malware	5 Genes | 1.18%
zlib	Library	33 Genes | 7.78%

File Metadata

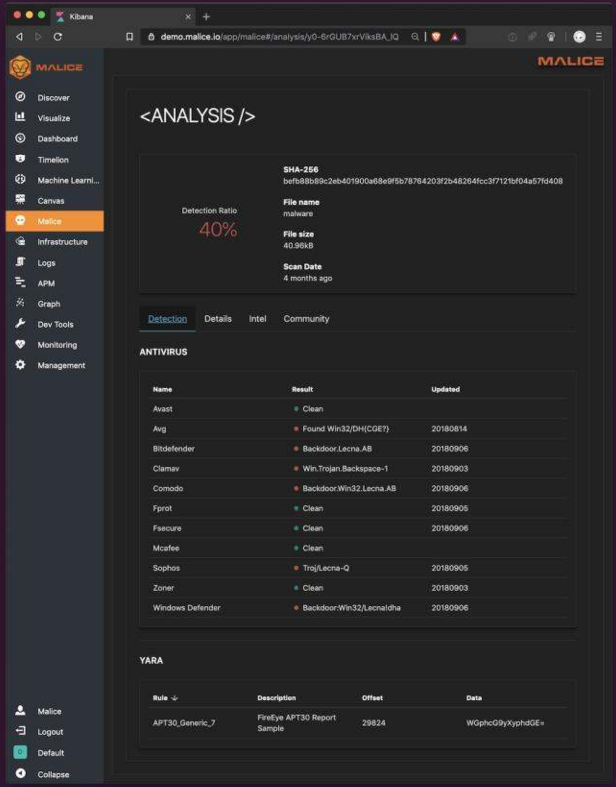
Size	240 KB
SHA256	[illegible]
MD5	[illegible]
Company	Microsoft Corporation (0 genes from "Microsoft Corporation")
Product	Microsoft Windows Operating System [illegible]
SHA1	[illegible]
ssdeep	[illegible]
virustotal	Report [illegible]
Target Machine	Intel 386 or later, and compatibles
Compilation Timestamp	14 Jul 2009

Malware Analysis

- Offline services
  - Repos and DB
    - viper
  - Sandboxes
    - Cuckoo
  - Classification
    - (IRMA), Malice, **VirusChecker**
  - **Remember, integrations and automatization**



```
+--------------+---------------------------------------------------------------------------------+
| Command      | Description                                                                     |
+--------------+---------------------------------------------------------------------------------+
| apk          | Parse Android Applications                                                      |
| clamav       | Scan file from local ClamAV daemon                                              |
| cuckoo       | Submit the file to Cuckoo Sandbox                                               |
| debup        | Parse McAfee BUP Files                                                          |
| editdistance | Edit distance on the filenames                                                  |
| elf          | Extract information from ELF headers                                            |
| email        | Parse eml and msg email files                                                   |
| exif         | Extract Exif MetaData                                                           |
| fuzzy        | Search for similar files through fuzzy hashing                                  |
| html         | Parse html files and extract content                                            |
| ida          | Start IDA Pro                                                                   |
| idx          | Parse Java IDX files                                                            |
| image        | Perform analysis on images                                                      |
| jar          | Parse Java JAR archives                                                         |
| koodous      | Interact with Koodous                                                           |
| lastline     | Submit files and retrieve reports from LastLine (default will print short summary) |
| macho        | Get Macho OSX Headers                                                           |
| misp         | Upload and query IOCs to/from a MISP instance                                   |
| office       | Office Document Parser                                                          |
| pdf          | Parse and analyze PDF documents                                                 |
| pdns         | Query a Passive DNS server                                                      |
| pe           | Extract information from PE32 headers                                           |
| pssl         | Query a Passive SSL server                                                      |
| pst          | Process PST Files for Attachment                                                |
| r2           | Start Radare2                                                                   |
| rat          | Extract information from known RAT families                                     |
| reports      | Online Sandboxes Reports                                                        |
| shellcode    | Search for known shellcode patterns                                             |
| size         | Size command to show/scan/cluster files                                         |
| strings      | Extract strings from file                                                       |
| swf          | Parse, analyze and decompress Flash objects                                     |
| triage       | Perform some initial triaging and tagging of the file                           |
```



<ANALYSIS />

Detection Ratio
40%

SHA-256
befb88b89c2eb401900a68e9f5b78764203f2b48264fcc3f7121bf04a57fd408

File name
malware

File size
40.96kB

Scan Date
4 months ago

Detection | Details | Intel | Community

ANTIVIRUS

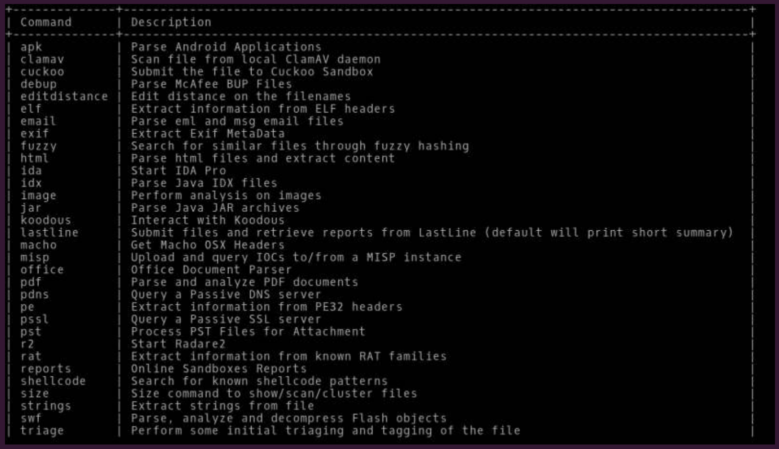
Name	Result	Updated
Avast	● Clean	
Avg	● Found Win32/DH{CGE?}	20180814
Bitdefender	● Backdoor.Lecna.AB	20180906
Clamav	● Win.Trojan.Backspace-1	20180903
Comodo	● Backdoor.Win32.Lecna.AB	20180906
Fprot	● Clean	20180905
Fsecure	● Clean	20180906
Mcafee	● Clean	
Sophos	● Troj/Lecna-Q	20180905
Zoner	● Clean	20180903
Windows Defender	● Backdoor:Win32/Lecna!dha	20180906

YARA

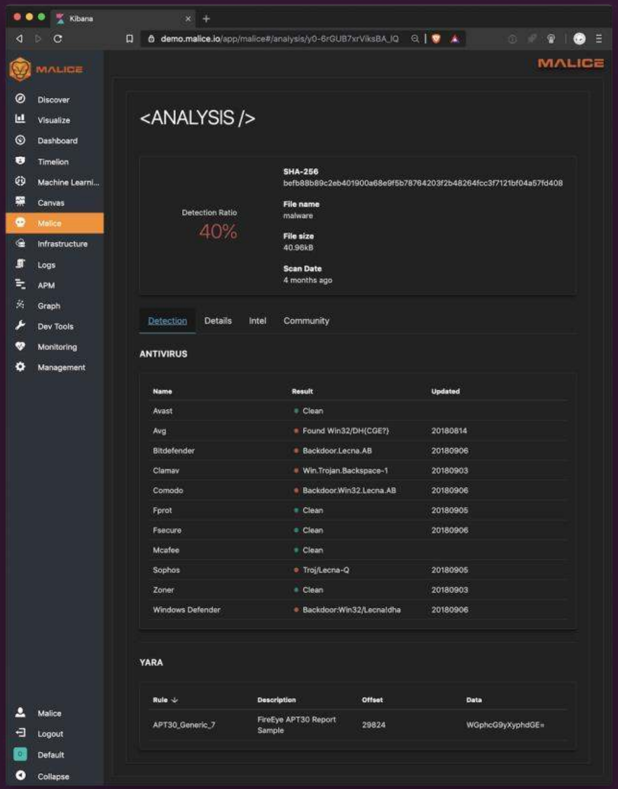
Rule ↓	Description	Offset	Data
APT30_Generic_7	FireEye APT30 Report Sample	29824	WGphcG9yXyphdGE=

Malware Analysis

- Offline services
  - Repos and DB
    - viper
  - Sandboxes
    - Cuckoo
  - Classification
    - (IRMA), Malice, **VirusChecker**
  - **Remember, integrations and automatization**



```
+--------------+------------------------------------------------------------------------------------+
| Command      | Description                                                                        |
+--------------+------------------------------------------------------------------------------------+
| apk          | Parse Android Applications                                                         |
| clamav       | Scan file from local ClamAV daemon                                                 |
| cuckoo       | Submit the file to Cuckoo Sandbox                                                  |
| debup        | Parse McAfee BUP Files                                                             |
| editdistance | Edit distance on the filenames                                                     |
| elf          | Extract information from ELF headers                                               |
| email        | Parse eml and msg email files                                                      |
| exif         | Extract Exif MetaData                                                              |
| fuzzy        | Search for similar files through fuzzy hashing                                     |
| html         | Parse html files and extract content                                               |
| ida          | Start IDA Pro                                                                      |
| idx          | Parse Java IDX files                                                               |
| image        | Perform analysis on images                                                         |
| jar          | Parse Java JAR archives                                                            |
| koodous      | Interact with Koodous                                                              |
| lastline     | Submit files and retrieve reports from LastLine (default will print short summary) |
| macho        | Get Macho OSX Headers                                                              |
| misp         | Upload and query IOCs to/from a MISP instance                                      |
| office       | Office Document Parser                                                             |
| pdf          | Parse and analyze PDF documents                                                    |
| pdns         | Query a Passive DNS server                                                         |
| pe           | Extract information from PE32 headers                                              |
| pssl         | Query a Passive SSL server                                                         |
| pst          | Process PST Files for Attachment                                                   |
| r2           | Start Radare2                                                                      |
| rat          | Extract information from known RAT families                                        |
| reports      | Online Sandboxes Reports                                                           |
| shellcode    | Search for known shellcode patterns                                                |
| size         | Size command to show/scan/cluster files                                            |
| strings      | Extract strings from file                                                          |
| swf          | Parse, analyze and decompress Flash objects                                        |
| triage       | Perform some initial triaging and tagging of the file                              |
```



<ANALYSIS />

Detection Ratio
40%

SHA-256
befb88b89c2eb401900a68e9f5b78764203f2b48264fcc3f7121bf04a57fd408

File name
malware

File size
40.96kB

Scan Date
4 months ago

ANTIVIRUS

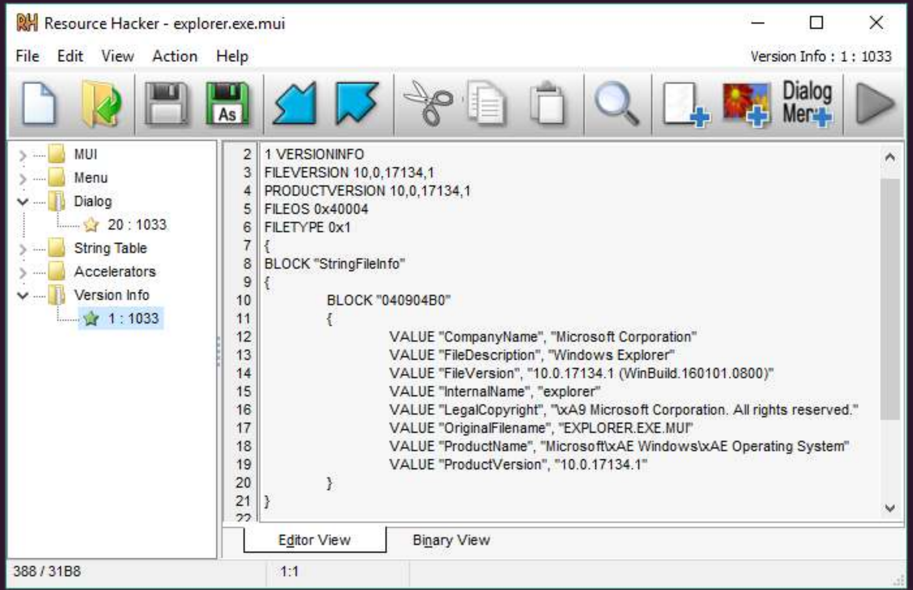
Name	Result	Updated
Avast	● Clean	
Avg	● Found Win32/DH{CGE?}	20180814
Bitdefender	● Backdoor.Lecna.AB	20180906
Clamav	● Win.Trojan.Backspace-1	20180903
Comodo	● Backdoor.Win32.Lecna.AB	20180906
Fprot	● Clean	20180905
Fsecure	● Clean	20180906
Mcafee	● Clean	
Sophos	● Troj/Lecna-Q	20180905
Zoner	● Clean	20180903
Windows Defender	● Backdoor:Win32/Lecna!dha	20180906

YARA

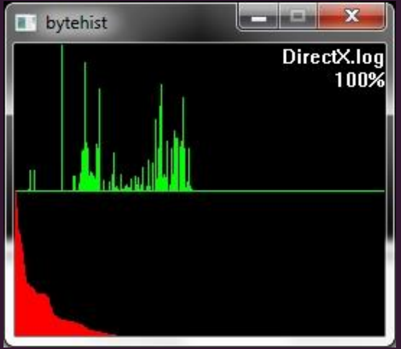
Rule ↓	Description	Offset	Data
APT30_Generic_7	FireEye APT30 Report Sample	29824	WGphcG9yXyphdGE=

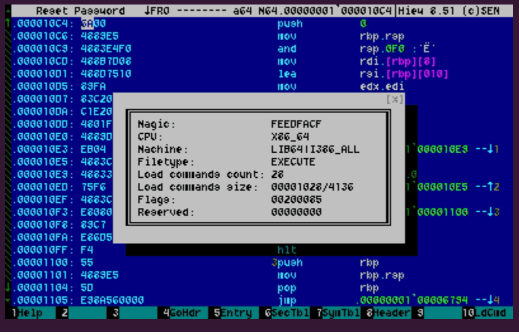
Malware Analysis

- Static analysis
  - PE Tools, oletools
  - PEStudio, Resource hacker
  - Strings (also strings –e l)
  - Bytehist, densityscout
  - CyberChef, xortool
  - Didier Stevens Suite
  - Hiew Demo
  - Far Manager + plugins
  - Binvis.io

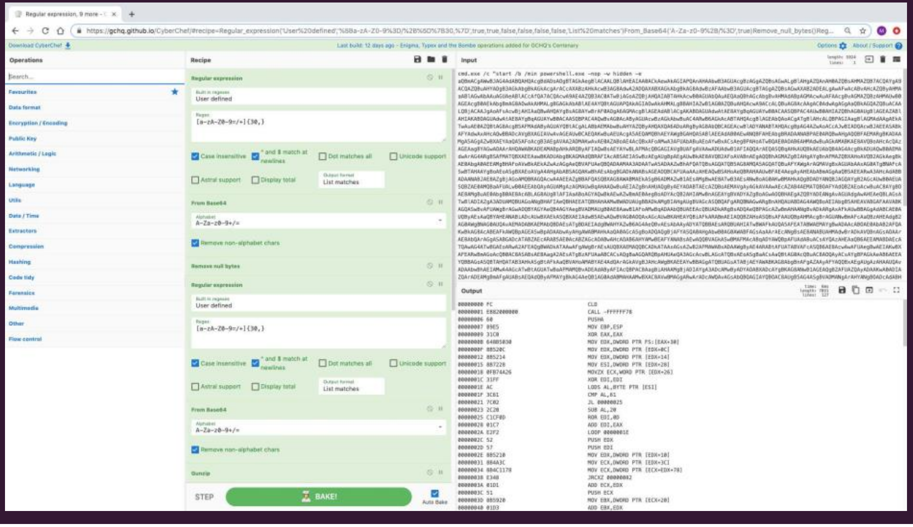


```
1 VERSIONINFO
FILEVERSION 10,0,17134,1
PRODUCTVERSION 10,0,17134,1
FILEOS 0x40004
FILETYPE 0x1
{
BLOCK "StringFileInfo"
{
        BLOCK "040904B0"
        {
                VALUE "CompanyName", "Microsoft Corporation"
                VALUE "FileDescription", "Windows Explorer"
                VALUE "FileVersion", "10.0.17134.1 (WinBuild.160101.0800)"
                VALUE "InternalName", "explorer"
                VALUE "LegalCopyright", "\xA9 Microsoft Corporation. All rights reserved."
                VALUE "OriginalFilename", "EXPLORER.EXE.MUI"
                VALUE "ProductName", "Microsoft\xAE Windows\xAE Operating System"
                VALUE "ProductVersion", "10.0.17134.1"
        }
}
```





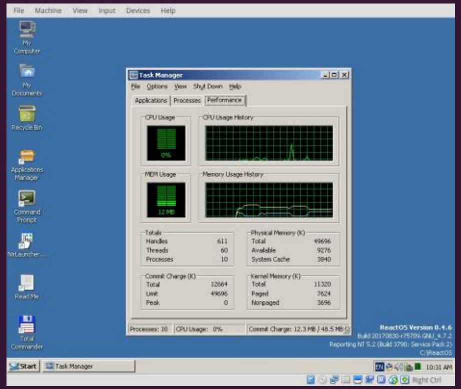
```
 Reset Password   ↓FRO -------- a64 M64.00000001`000010C4 |Hiew 8.51 (c)SEN
.000010C4: 6A00                          push    0
.000010C6: 4889E5                        mov     rbp,rsp
.000010C9: 4883E4F0                      and     rsp,0F0 ;'Ë'
.000010CD: 488B7D08                      mov     rdi,[rbp][8]
.000010D1: 488D7510                      lea     rsi,[rbp][010]
.000010D5: 89FA                          mov     edx,edi
.000010D7: 83C20
.000010DA: C1E20
.000010DD: 4801F
.000010E0: 4889D
.000010E3: EB04                                          1`000010E9 --↓1
.000010E5: 4883C
.000010E9: 48833                                         .0
.000010ED: 75F6                                          1`000010E5 --↑2
.000010EF: 4883C
.000010F3: E8080                                         1`00001100 --↓3
.000010F8: 89C7
.000010FA: E86D5
.000010FF: F4                            hlt
.00001100: 55                           3push    rbp
.00001101: 4889E5                        mov     rbp,rsp
.00001104: 5D                            pop     rbp
.00001105: E98A560000                    jmp     .00000001`00006794 --↓4

  Magic:                   FEEDFACF
  CPU:                     X86_64
  Machine:                 LIB64|I386_ALL
  Filetype:                EXECUTE
  Load commands count:     28
  Load commands size:      00001028/4136
  Flags:                   00200085
  Reserved:                00000000
```

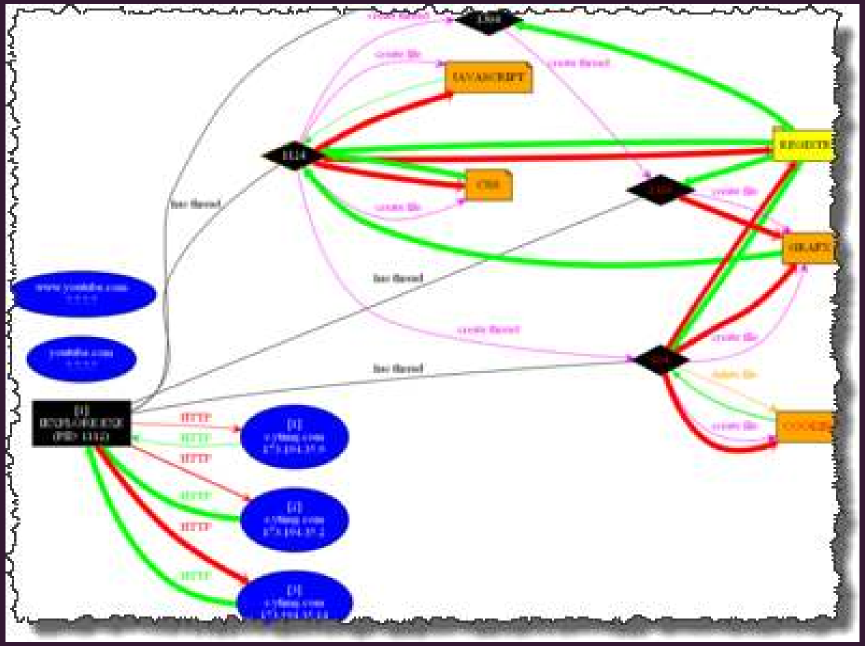


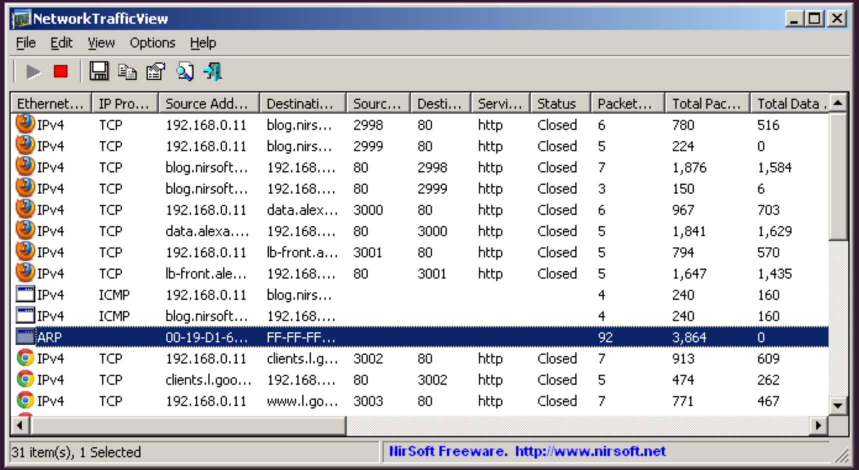
```
cmd.exe /c "start /b /min powershell.exe -nop -w hidden -e
```

Malware Analysis

- Behavioral analysis
  - VirtualBox, Qemu
    - ReactOS, modern.ie
  - inetsim, dnsmasq, FakeNet-NG
  - SysInternals (procmon, sysmon)
  - NirSoft (NetworkTrafficView, …)
  - WireShark, Burp
  - procdot



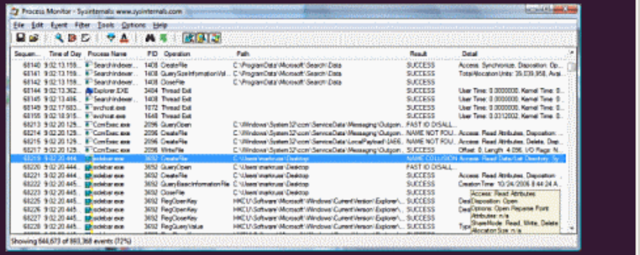




Ethernet...	IP Pro...	Source Add...	Destinati...	Sourc...	Desti...	Servi...	Status	Packet...	Total Pac...	Total Data ...
IPv4	TCP	192.168.0.11	blog.nirs...	2998	80	http	Closed	6	780	516
IPv4	TCP	192.168.0.11	blog.nirs...	2999	80	http	Closed	5	224	0
IPv4	TCP	blog.nirsoft...	192.168....	80	2998	http	Closed	7	1,876	1,584
IPv4	TCP	blog.nirsoft...	192.168....	80	2999	http	Closed	3	150	6
IPv4	TCP	192.168.0.11	data.alex...	3000	80	http	Closed	6	967	703
IPv4	TCP	data.alexa....	192.168....	80	3000	http	Closed	5	1,841	1,629
IPv4	TCP	192.168.0.11	lb-front.a...	3001	80	http	Closed	5	794	570
IPv4	TCP	lb-front.ale...	192.168....	80	3001	http	Closed	5	1,647	1,435
IPv4	ICMP	192.168.0.11	blog.nirs...					4	240	160
IPv4	ICMP	blog.nirsoft...	192.168....					4	240	160
ARP		00-19-D1-6...	FF-FF-FF...					92	3,864	0
IPv4	TCP	192.168.0.11	clients.l.g...	3002	80	http	Closed	7	913	609
IPv4	TCP	clients.l.goo...	192.168....	80	3002	http	Closed	5	474	262
IPv4	TCP	192.168.0.11	www.l.go...	3003	80	http	Closed	7	771	467

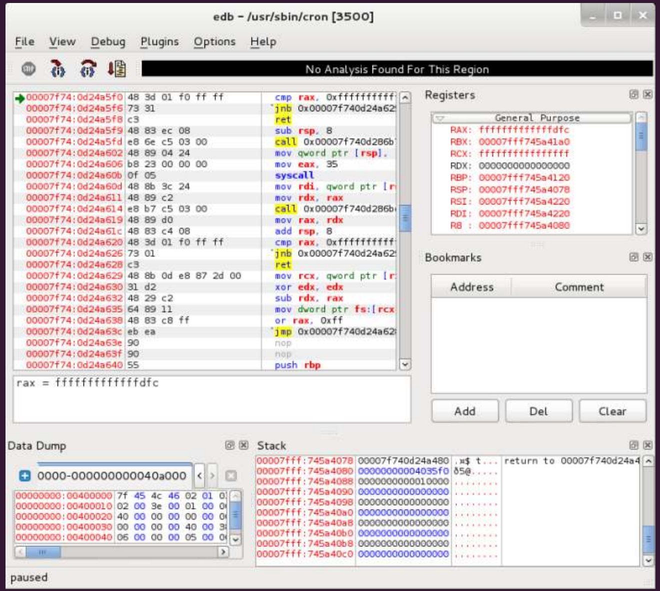
31 item(s), 1 Selected

NirSoft Freeware. http://www.nirsoft.net



Malware Analysis

- Debugging
  - Gdb-dashboard, edb
  - WinDbg, Immunity debugger
    - Mona
  - x64dbg

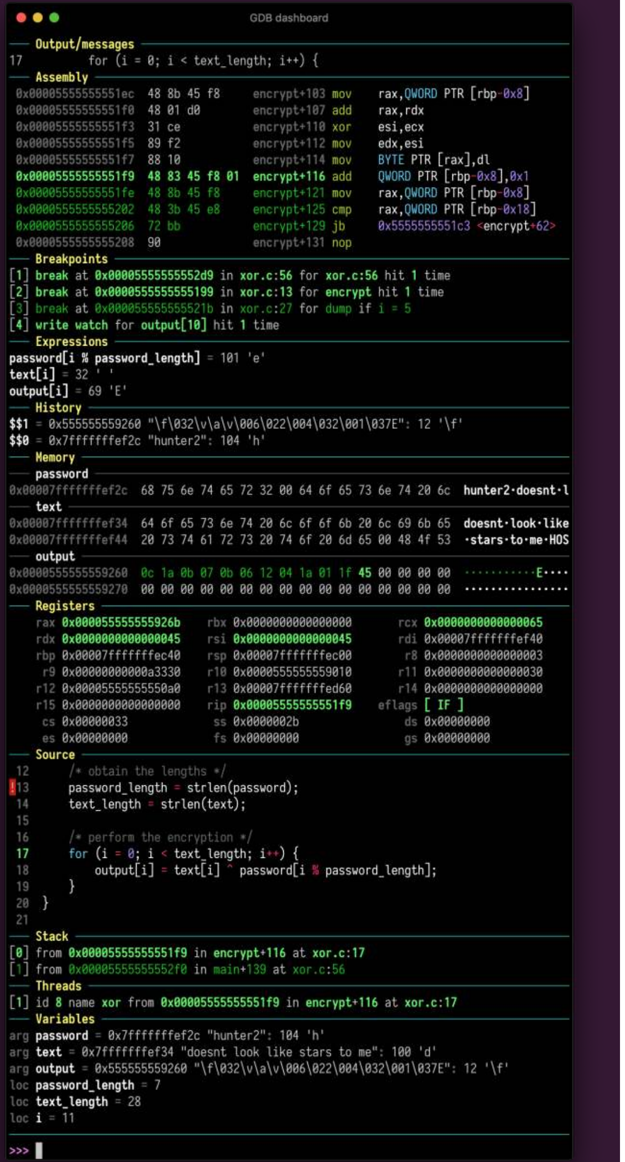


```
00007f74:0d24a5f0 48 3d 01 f0 ff ff      cmp rax, 0xffffffffff
00007f74:0d24a5f6 73 31                  jnb 0x00007f740d24a62
00007f74:0d24a5f8 c3                     ret
00007f74:0d24a5f9 48 83 ec 08            sub rsp, 8
00007f74:0d24a5fd e8 6e c5 03 00         call 0x00007f740d286b
00007f74:0d24a602 48 89 04 24            mov qword ptr [rsp],
00007f74:0d24a606 b8 23 00 00 00         mov eax, 35
00007f74:0d24a60b 0f 05                  syscall
00007f74:0d24a60d 48 8b 3c 24            mov rdi, qword ptr [r
00007f74:0d24a611 48 89 c2               mov rdx, rax
00007f74:0d24a614 e8 b7 c5 03 00         call 0x00007f740d286b
00007f74:0d24a619 48 89 d0               mov rax, rdx
00007f74:0d24a61c 48 83 c4 08            add rsp, 8
00007f74:0d24a620 48 3d 01 f0 ff ff      cmp rax, 0xffffffffff
00007f74:0d24a626 73 01                  jnb 0x00007f740d24a62
00007f74:0d24a628 c3                     ret
00007f74:0d24a629 48 8b 0d e8 87 2d 00   mov rcx, qword ptr [r
00007f74:0d24a630 31 d2                  xor edx, edx
00007f74:0d24a632 48 29 c2               sub rdx, rax
00007f74:0d24a635 64 89 11               mov dword ptr fs:[rcx
00007f74:0d24a638 48 83 c8 ff            or rax, 0xff
00007f74:0d24a63c eb ea                  jmp 0x00007f740d24a62
00007f74:0d24a63e 90                     nop
00007f74:0d24a63f 90                     nop
00007f74:0d24a640 55                     push rbp

rax = fffffffffffffdfc
```

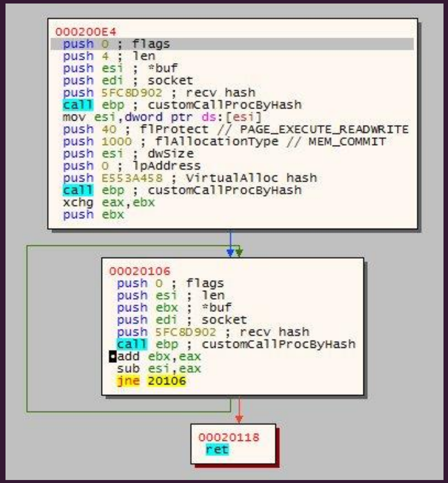
```
RAX: fffffffffffffdfc
RBX: 00007fff745a41a0
RCX: ffffffffffffffff
RDX: 0000000000000000
RBP: 00007fff745a4120
RSP: 00007fff745a4078
RSI: 00007fff745a4220
RDI: 00007fff745a4220
R8 : 00007fff745a4080
```

```
0000-000000000040a000
00000000:00400000 7f 45 4c 46 02 01 0
00000000:00400010 02 00 3e 00 01 00 0
00000000:00400020 40 00 00 00 00 00 0
00000000:00400030 00 00 00 00 40 00 3
00000000:00400040 06 00 00 00 05 00 0
```

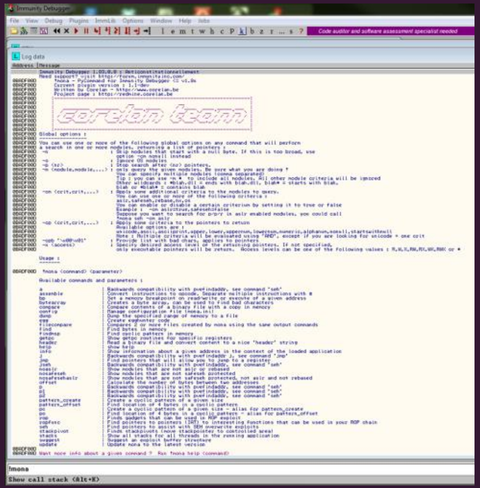
```
00007fff:745a4078 00007f740d24a480 .¤$ t... return to 00007f740d24a4
00007fff:745a4080 00000000004035f0 ð5@.....
00007fff:745a4088 0000000000010000 ........
00007fff:745a4090 0000000000000000 ........
00007fff:745a4098 0000000000000000 ........
00007fff:745a40a0 0000000000000000 ........
00007fff:745a40a8 0000000000000000 ........
00007fff:745a40b0 0000000000000000 ........
00007fff:745a40b8 0000000000000000 ........
00007fff:745a40c0 0000000000000000 ........
```



```
── Output/messages ─────────────────────────────────────────────
17          for (i = 0; i < text_length; i++) {
── Assembly ────────────────────────────────────────────────────
 0x00005555555551ec  48 8b 45 f8     encrypt+103 mov   rax,QWORD PTR [rbp-0x8]
 0x00005555555551f0  48 01 d0        encrypt+107 add   rax,rdx
 0x00005555555551f3  31 ce           encrypt+110 xor   esi,ecx
 0x00005555555551f5  89 f2           encrypt+112 mov   edx,esi
 0x00005555555551f7  88 10           encrypt+114 mov   BYTE PTR [rax],dl
 0x00005555555551f9  48 83 45 f8 01  encrypt+116 add   QWORD PTR [rbp-0x8],0x1
 0x00005555555551fe  48 8b 45 f8     encrypt+121 mov   rax,QWORD PTR [rbp-0x8]
 0x0000555555555202  48 3b 45 e8     encrypt+125 cmp   rax,QWORD PTR [rbp-0x18]
 0x0000555555555206  72 bb           encrypt+129 jb    0x5555555551c3 <encrypt+62>
 0x0000555555555208  90              encrypt+131 nop
── Breakpoints ─────────────────────────────────────────────────
[1] break at 0x00005555555552d9 in xor.c:56 for xor.c:56 hit 1 time
[2] break at 0x0000555555555199 in xor.c:13 for encrypt hit 1 time
[3] break at 0x000055555555521b in xor.c:27 for dump if i = 5
[4] write watch for output[10] hit 1 time
── Expressions ─────────────────────────────────────────────────
password[i % password_length] = 101 'e'
text[i] = 32 ' '
output[i] = 69 'E'
── History ─────────────────────────────────────────────────────
$$1 = 0x555555559260 "\f\032\v\a\v\006\022\004\032\001\037E": 12 '\f'
$$0 = 0x7fffffffef2c "hunter2": 104 'h'
── Memory ──────────────────────────────────────────────────────
── password ────────────────────────────────────────────────────
0x00007fffffffef2c  68 75 6e 74 65 72 32 00 64 6f 65 73 6e 74 20 6c  hunter2·doesnt·l
── text ────────────────────────────────────────────────────────
0x00007fffffffef34  64 6f 65 73 6e 74 20 6c 6f 6f 6b 20 6c 69 6b 65  doesnt·look·like
0x00007fffffffef44  20 73 74 61 72 73 20 74 6f 20 6d 65 00 48 4f 53  ·stars·to·me·HOS
── output ──────────────────────────────────────────────────────
0x0000555555559260  0c 1a 0b 07 0b 06 12 04 1a 01 1f 45 00 00 00 00  ···········E····
0x0000555555559270  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ················
── Registers ───────────────────────────────────────────────────
   rax 0x000055555555926b    rbx 0x0000000000000000    rcx 0x0000000000000065
   rdx 0x0000000000000045    rsi 0x0000000000000045    rdi 0x00007fffffffef40
   rbp 0x00007fffffffec40    rsp 0x00007fffffffec00     r8 0x0000000000000003
    r9 0x00000000000a3330    r10 0x0000555555559010    r11 0x0000000000000030
   r12 0x00005555555550a0    r13 0x00007fffffffed60    r14 0x0000000000000000
   r15 0x0000000000000000    rip 0x00005555555551f9 eflags [ IF ]
    cs 0x00000033             ss 0x0000002b             ds 0x00000000
    es 0x00000000             fs 0x00000000             gs 0x00000000
── Source ──────────────────────────────────────────────────────
 12       /* obtain the lengths */
!13       password_length = strlen(password);
 14       text_length = strlen(text);
 15
 16       /* perform the encryption */
 17       for (i = 0; i < text_length; i++) {
 18           output[i] = text[i] ^ password[i % password_length];
 19       }
 20   }
 21
── Stack ───────────────────────────────────────────────────────
[0] from 0x00005555555551f9 in encrypt+116 at xor.c:17
[1] from 0x00005555555552f0 in main+139 at xor.c:56
── Threads ─────────────────────────────────────────────────────
[1] id 8 name xor from 0x00005555555551f9 in encrypt+116 at xor.c:17
── Variables ───────────────────────────────────────────────────
arg password = 0x7fffffffef2c "hunter2": 104 'h'
arg text = 0x7fffffffef34 "doesnt look like stars to me": 100 'd'
arg output = 0x555555559260 "\f\032\v\a\v\006\022\004\032\001\037E": 12 '\f'
loc password_length = 7
loc text_length = 28
loc i = 11
────────────────────────────────────────────────────────────────
>>>
```



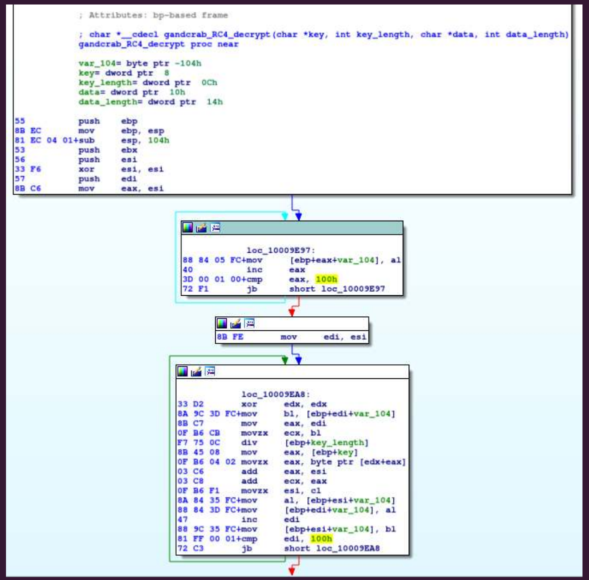
```
000200E4
 push 0 ; flags
 push 4 ; len
 push esi ; *buf
 push edi ; socket
 push 5FC8D902 ; recv hash
 call ebp ; customCallProcByHash
 mov esi,dword ptr ds:[esi]
 push 40 ; flProtect // PAGE_EXECUTE_READWRITE
 push 1000 ; flAllocationType // MEM_COMMIT
 push esi ; dwSize
 push 0 ; lpAddress
 push E553A458 ; VirtualAlloc hash
 call ebp ; customCallProcByHash
 xchg eax,ebx
 push ebx

00020106
 push 0 ; flags
 push esi ; len
 push ebx ; *buf
 push edi ; socket
 push 5FC8D902 ; recv hash
 call ebp ; customCallProcByHash
 add ebx,eax
 sub esi,eax
 jne 20106

00020118
 ret
```



```
Immunity Debugger 1.83.0.0 : Anticonstitutionellement
Need support? visit http://forum.immunityinc.com/
0BADF00D      !mona - PyCommand for Immunity Debugger <= v1.8x
0BADF00D      Current plugin version : 1.1-dev
0BADF00D      Written by Corelan - https://www.corelan.be
0BADF00D      Project page : https://redmine.corelan.be
0BADF00D Global options :
0BADF00D You can use one or more of the following global options on any command that will perform
0BADF00D a search in one or more modules, returning a list of pointers :
0BADF00D  -n                      : Skip modules that start with a null byte. If this is too broad, use
0BADF00D                            option -cm nonull instead
0BADF00D  -o                      : Ignore OS modules
0BADF00D  -p <nr>                 : Stop search after <nr> pointers.
0BADF00D  -m <module,module,...>  : only query the given modules. Be sure what you are doing !
0BADF00D                            You can specify multiple modules (comma separated)
0BADF00D  -cm <crit,crit,...>     : Apply some additional criteria to the modules to query.
0BADF00D  -cp <crit,crit,...>     : Apply some criteria to the pointers to return
0BADF00D  -cpb "\x00\x0a"         : Provide list with bad chars, applies to pointers
0BADF00D  -x <access>             : Specify desired access level of the returning pointers. If not specified,
Usage :
0BADF00D  !mona <command> <parameter>
Available commands and parameters :
a             | Backwards compatibility with pvefindaddr, see command "seh"
assemble      | Convert instructions to opcode. Separate multiple instructions with #
bp            | Set a memory breakpoint on read/write or execute of a given address
bytearray     | Creates a byte array, can be used to find bad characters
compare       | Compare contents of a binary file with a copy in memory
config        | Manage configuration file (mona.ini)
```

Malware Analysis

- Reverse-engineering
  - Radare2 + Cutter, Ghidra
  - Hopper, Binary Ninja
  - Ida 7.0 Freeware
  - Snowman decompiler
  - Mono Develop, ILSpy, dnSpy, de4dot
  - jd-gui, bytecodeviewer
  - Beautifier.io, onlinedisassembler.com

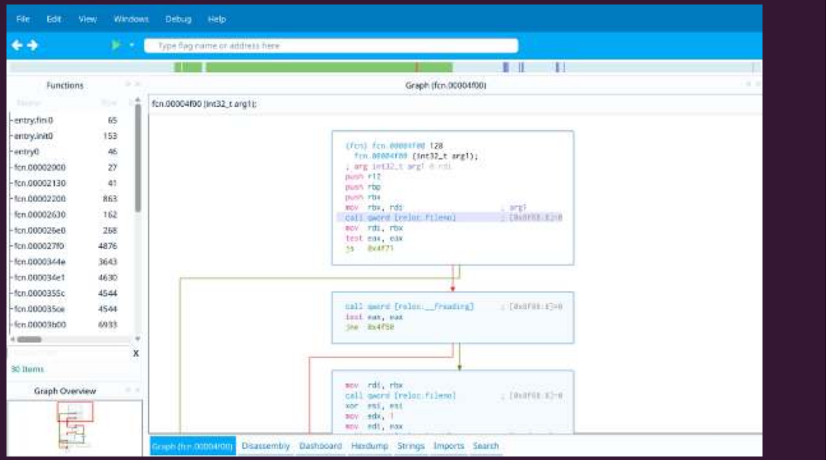


```
; Attributes: bp-based frame

; char *__cdecl gandcrab_RC4_decrypt(char *key, int key_length, char *data, int data_length)
gandcrab_RC4_decrypt proc near

var_104= byte ptr -104h
key= dword ptr  8
key_length= dword ptr  0Ch
data= dword ptr  10h
data_length= dword ptr  14h

55          push    ebp
8B EC       mov     ebp, esp
81 EC 04 01+sub     esp, 104h
53          push    ebx
56          push    esi
33 F6       xor     esi, esi
57          push    edi
8B C6       mov     eax, esi
```

```
            loc_10009E97:
88 84 05 FC+mov     [ebp+eax+var_104], al
40          inc     eax
3D 00 01 00+cmp     eax, 100h
72 F1       jb      short loc_10009E97
```

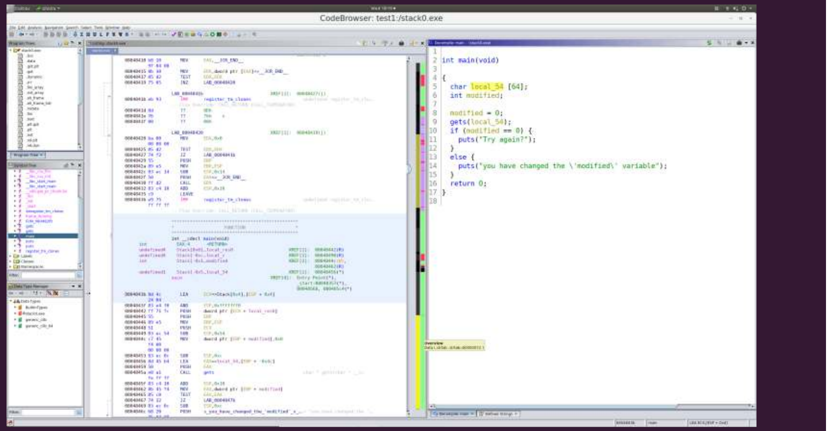
```
8B FE       mov     edi, esi
```

```
            loc_10009EA8:
33 D2       xor     edx, edx
8A 9C 3D FC+mov     bl, [ebp+edi+var_104]
8B C7       mov     eax, edi
0F B6 CB    movzx   ecx, bl
F7 75 0C    div     [ebp+key_length]
8B 45 08    mov     eax, [ebp+key]
0F B6 04 02 movzx   eax, byte ptr [edx+eax]
03 C6       add     eax, esi
03 C8       add     ecx, eax
0F B6 F1    movzx   esi, cl
8A 84 35 FC+mov     al, [ebp+esi+var_104]
88 84 3D FC+mov     [ebp+edi+var_104], al
47          inc     edi
88 9C 35 FC+mov     [ebp+esi+var_104], bl
81 FF 00 01+cmp     edi, 100h
72 C3       jb      short loc_10009EA8
```



```
entry.fini0       65
entry.init0      153
entry0            46
fcn.00002000      27
fcn.00002130      41
fcn.00002200     863
fcn.00002630     162
fcn.000026e0     268
fcn.000027f0    4876
fcn.0000344e    3643
fcn.000034e1    4630
fcn.0000355c    4544
fcn.000035ce    4544
fcn.00003b00    6933
```

```
fcn.00004f00 (int32_t arg1);

(fcn) fcn.00004f00 128
  fcn.00004f00 (int32_t arg1);
; arg int32_t arg1 @ rdi
push r12
push rbp
push rbx
mov  rbx, rdi                     ; arg1
call qword [reloc.fileno]
mov  rdi, rbx
test eax, eax
js   0x4f71

call qword [reloc.__freading]
test eax, eax
jne  0x4f58

mov  rdi, rbx
call qword [reloc.fileno]
xor  esi, esi
mov  edx, 1
mov  edi, eax
```

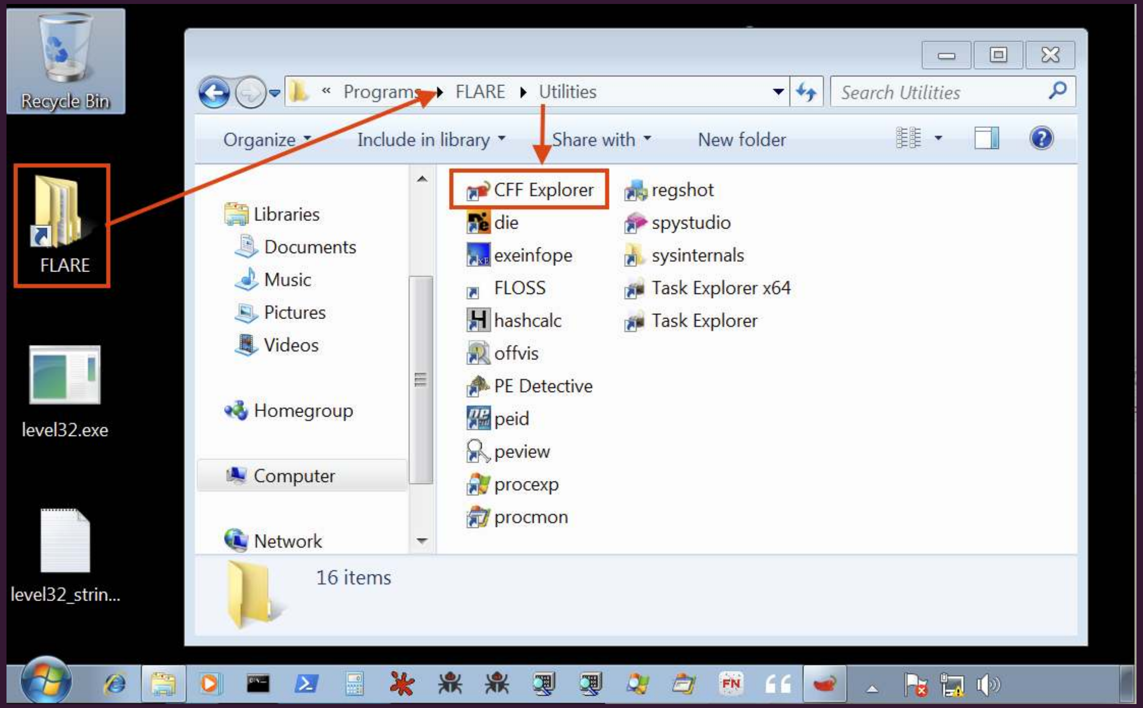


CodeBrowser: test1:/stack0.exe

```
int main(void)

{
  char local_54 [64];
  int modified;

  modified = 0;
  gets(local_54);
  if (modified == 0) {
    puts("Try again?");
  }
  else {
    puts("you have changed the \'modified\' variable");
  }
  return 0;
}
```

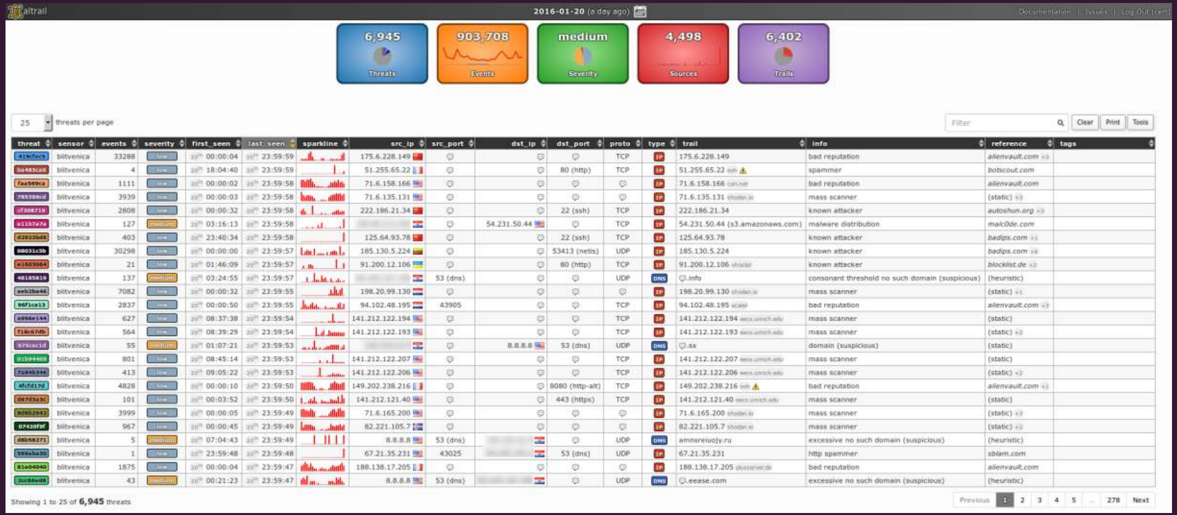
Malware Analysis

- Distributions, OS
  - REMnux
  - Flare-vm



Monitoring, detection

- Plenty of tools
  - IDS,IPS, SIEM
    - Suricata, Zeek (Bro), Snort, AlienVault OSSIM, SIEMonster, Elastic
  - Packate capture and analysis
    - Molo.ch, SiLK, Malcolm
  - Malicious traffic detection
    - Maltrail
  - Log processing and correlation
    - sec (perl)



threat	sensor	events	severity	first_seen	last_seen	sparkline	src_ip	src_port	dst_ip	dst_port	proto	type	trail	info	reference	tags
419dfec5	blitvenica	33288	low	20th 00:00:04	20th 23:59:59		175.6.228.149				TCP	IP	175.6.228.149	bad reputation	alienvault.com +3	
5a483ca0	blitvenica	4	low	20th 18:04:40	20th 23:59:59		51.255.65.22			80 (http)	TCP	IP	51.255.65.22 ovh ⚠	spammer	botscout.com	
faa569ca	blitvenica	1111	low	20th 00:00:02	20th 23:59:58		71.6.158.166					IP	71.6.158.166 cari.net	bad reputation	alienvault.com	
785399cd	blitvenica	3939	low	20th 00:00:03	20th 23:59:58		71.6.135.131					IP	71.6.135.131 shodan.io	mass scanner	(static) +3	
cf508719	blitvenica	2808	low	20th 00:00:32	20th 23:59:58		222.186.21.34			22 (ssh)	TCP	IP	222.186.21.34	known attacker	autoshun.org +3	
e11b7a7a	blitvenica	127	medium	20th 03:16:13	20th 23:59:58		[redacted]		54.231.50.44		TCP	IP	54.231.50.44 (s3.amazonaws.com)	malware distribution	malc0de.com	
d2923bd8	blitvenica	403	low	20th 23:40:34	20th 23:59:58		125.64.93.78			22 (ssh)	TCP	IP	125.64.93.78	known attacker	badips.com +1	
08031c3b	blitvenica	30298	low	20th 00:00:00	20th 23:59:57		185.130.5.224			53413 (netis)	UDP	IP	185.130.5.224	known attacker	badips.com +6	
e1683864	blitvenica	21	low	20th 01:46:09	20th 23:59:57		91.200.12.106			80 (http)	TCP	IP	91.200.12.106 shodan	known attacker	blocklist.de +2	
48185819	blitvenica	137	medium	20th 03:24:55	20th 23:59:57		[redacted]	53 (dns)			UDP	DNS	.info	consonant threshold no such domain (suspicious)	(heuristic)	
aeb2ba46	blitvenica	7082	low	20th 00:00:32	20th 23:59:55		198.20.99.130					IP	198.20.99.130 shodan.io	mass scanner	(static) +1	
96f1ca13	blitvenica	2837	low	20th 00:00:50	20th 23:59:55		94.102.48.195	43905			TCP	IP	94.102.48.195	bad reputation	alienvault.com +3	
a996e144	blitvenica	627	low	20th 08:37:38	20th 23:59:54		141.212.122.194				TCP	IP	141.212.122.194 eecs.umich.edu	mass scanner	(static)	
f18c67db	blitvenica	564	low	20th 08:39:29	20th 23:59:54		141.212.122.193				TCP	IP	141.212.122.193 eecs.umich.edu	mass scanner	(static) +1	
97bcac1d	blitvenica	55	medium	20th 01:07:21	20th 23:59:53		[redacted]		8.8.8.8	53 (dns)	UDP	DNS	.sx	domain (suspicious)	(static)	
01b94405	blitvenica	801	low	20th 08:45:14	20th 23:59:53		141.212.122.207				TCP	IP	141.212.122.207 eecs.umich.edu	mass scanner	(static)	
7a84b346	blitvenica	413	low	20th 09:05:22	20th 23:59:53		141.212.122.206				TCP	IP	141.212.122.206 eecs.umich.edu	mass scanner	(static) +1	
4fcfd17d	blitvenica	4828	low	20th 00:00:10	20th 23:59:50		149.202.238.216			8080 (http-alt)	TCP	IP	149.202.238.216 ovh ⚠	bad reputation	alienvault.com +1	
d67d3a3c	blitvenica	101	low	20th 00:03:52	20th 23:59:50		141.212.121.40			443 (https)	TCP	IP	141.212.121.40 eecs.umich.edu	mass scanner	(static)	
8d8b2642	blitvenica	3999	low	20th 00:00:05	20th 23:59:49		71.6.165.200					IP	71.6.165.200 shodan.io	mass scanner	(static) +3	
07420f9f	blitvenica	967	low	20th 00:00:45	20th 23:59:49		82.221.105.7					IP	82.221.105.7 shodan.io	mass scanner	(static) +1	
d8b58271	blitvenica	5	medium	20th 07:04:43	20th 23:59:49		8.8.8.8	53 (dns)	[redacted]		UDP	DNS	amnsreiuojy.ru	excessive no such domain (suspicious)	(heuristic)	
569aba30	blitvenica	1	low	20th 23:59:48	20th 23:59:48		67.21.35.231	43025	[redacted]	53 (dns)	UDP	IP	67.21.35.231	http spammer	sblam.com	
81e04040	blitvenica	1875	low	20th 00:00:04	20th 23:59:47		188.138.17.205					IP	188.138.17.205	bad reputation	alienvault.com	
2cc66ed8	blitvenica	43	medium	20th 00:21:23	20th 23:59:47		8.8.8.8	53 (dns)	[redacted]		UDP	DNS	.eease.com	excessive no such domain (suspicious)	(heuristic)	

Showing 1 to 25 of **6,945** threats

What next?

- And many more tools
  - Pentesting, auditing, …
- For beginning, don’t need to have everything
  - Start with incident handling and scale-up
  - Quality > quantity (feeds, tools,…)
- **Context**
  - Focus on relevant risk
  - Increased efficiency => better security

References, picture sources

- https://www.zimbra.com/open-source-email-overview/
- https://mattermost.com/
- https://etherpad.org/
- https://kanboard.org/
- https://signal.org/
- https://en.wikipedia.org/wiki/OTRS
- https://go.demisto.com/hs-fs/hubfs/demisto-thank%20you/banner_img.png
- https://github.com/TheHive-Project/TheHive
- https://github.com/NCSC-NL/taranis3/wiki/Admin-Configure-Software-Hardware
- https://www.misp-project.org/features.html

References, picture sources

- https://www.paterva.com/buy/maltego-clients/maltego-ce.php
- https://warden.cesnet.cz/cs/architecture
- https://www.opencti.io/en/
- https://go.recordedfuture.com/cyber-daily
- https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns
- https://digital-forensics.sans.org/blog/2009/06/18/forensics-101-acquiring-an-image-with-ftk-imager/
- https://www.youtube.com/watch?v=8u5HEE-JM74
- https://github.com/google/grr
- https://www.intezer.com/wp-content/uploads/2018/08/Wannacry-Small.png

References, picture sources

- https://any.run/img/screens/screenhd-real.png
- https://github.com/maliceio/malice
- https://github.com/CSIRT-SK/ioc-server
- https://github.com/CSIRT-SK/viruschecker
- https://www.circl.lu/assets/files/misp-training/luxembourg2017/4.2-viper.pdf
- https://twitter.com/mattnotmax/status/1122107157082558465
- https://cert.at/downloads/software/bytehist_en.html
- http://www.angusj.com/resourcehacker/
- http://www.hiew.ru/
- https://twitter.com/ladislav_b/status/914886748727054338

References, picture sources

- https://www.nirsoft.net/utils/network_traffic_view.html
- https://docs.microsoft.com/en-us/sysinternals/downloads/procmon
- https://www.procdot.com/onlinedocumentation.htm
- https://tools.kali.org/reverse-engineering/edb-debugger
- https://github.com/cyrus-and/gdb-dashboard
- https://twitter.com/ladislav_b/status/955708992155799552
- https://www.corelan.be/index.php/2011/07/14/mona-py-the-manual/
- https://cutter.re/
- https://github.com/NationalSecurityAgency/ghidra/issues/76
- https://www.fireeye.com/blog/threat-research/2017/07/flare-vm-the-windows-malware.html

Thank you

- Is that all? Finished, already?

- No, it's just the beginning :-)