Mason Competitive Cyber

From XML to IoCs: Rapid DFIR

What We're Discussing

- A Digital Forensics Methodology
  - Based largely on exp. at Crypsis
- Applicable to a variety of contexts
  - Mixed artifacts (event logs etc)
  - Linux (sort of)
  - Disk images
- Fast enough to use in CTFs
- Developable enough to use at work

Club PSAs

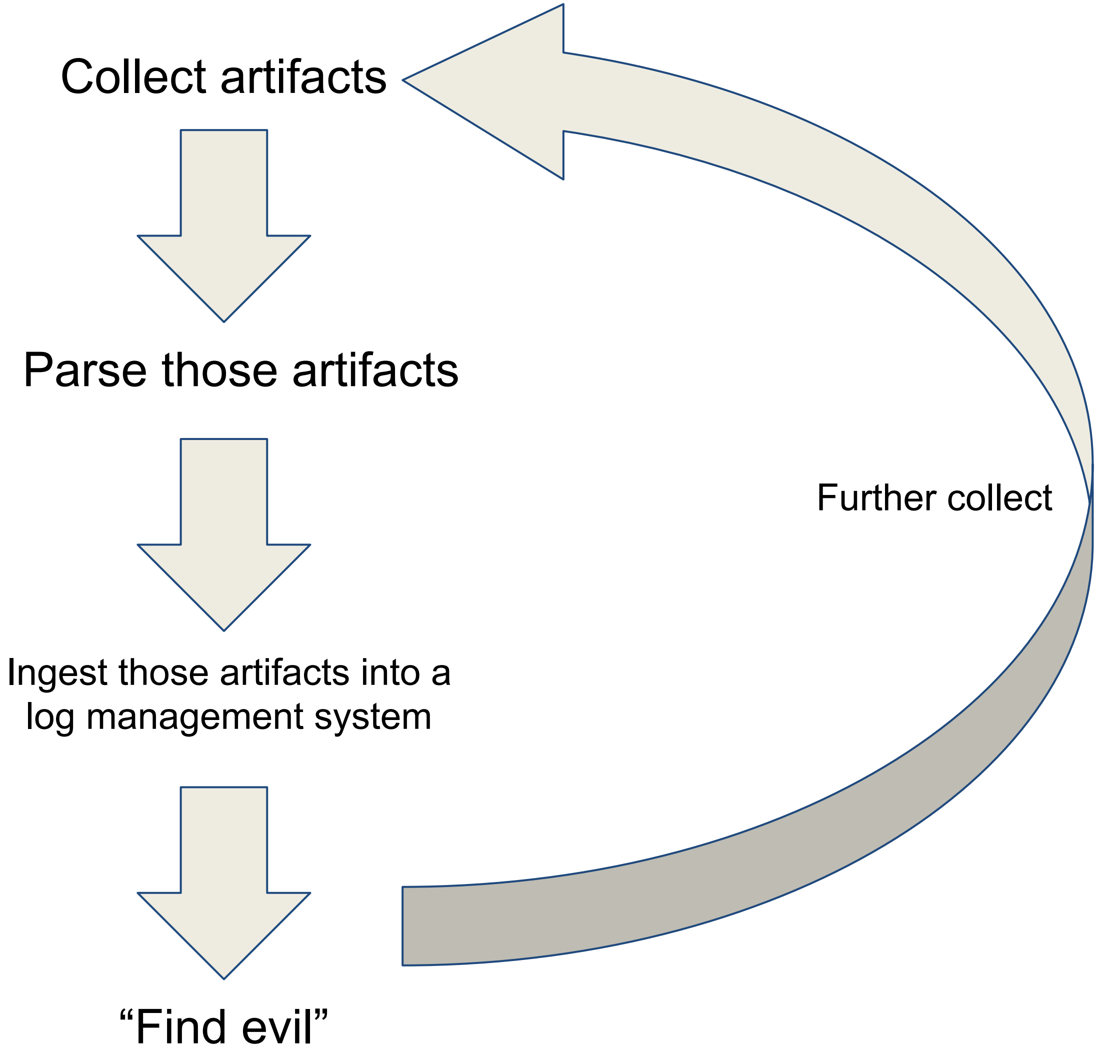
- patriotCTF
- CCDC Tryouts
- UVA CTFing

Hold for Qs

Crypsis

- Companies pay us for talks
  - It’s not as evil as it sounds
  - Company quality controls, meeting controls, etc
- Companies want to hire you
- **The Crypsis Group**
  - Digital Forensics and Incident Response
  - Fun not-quite-startup in Tysons
  - Accepts for a **ton** of roles - dev’ing, cases, etc
  - Accepts for full time and intern
- I work for Crypsis (2+ yrs)
  - Junior Security Engineer
- I’ve interviewed candidates for Crypsis

The Short of It: Free Stack



Collect artifacts

Parse those artifacts

Ingest those artifacts into a
log management system

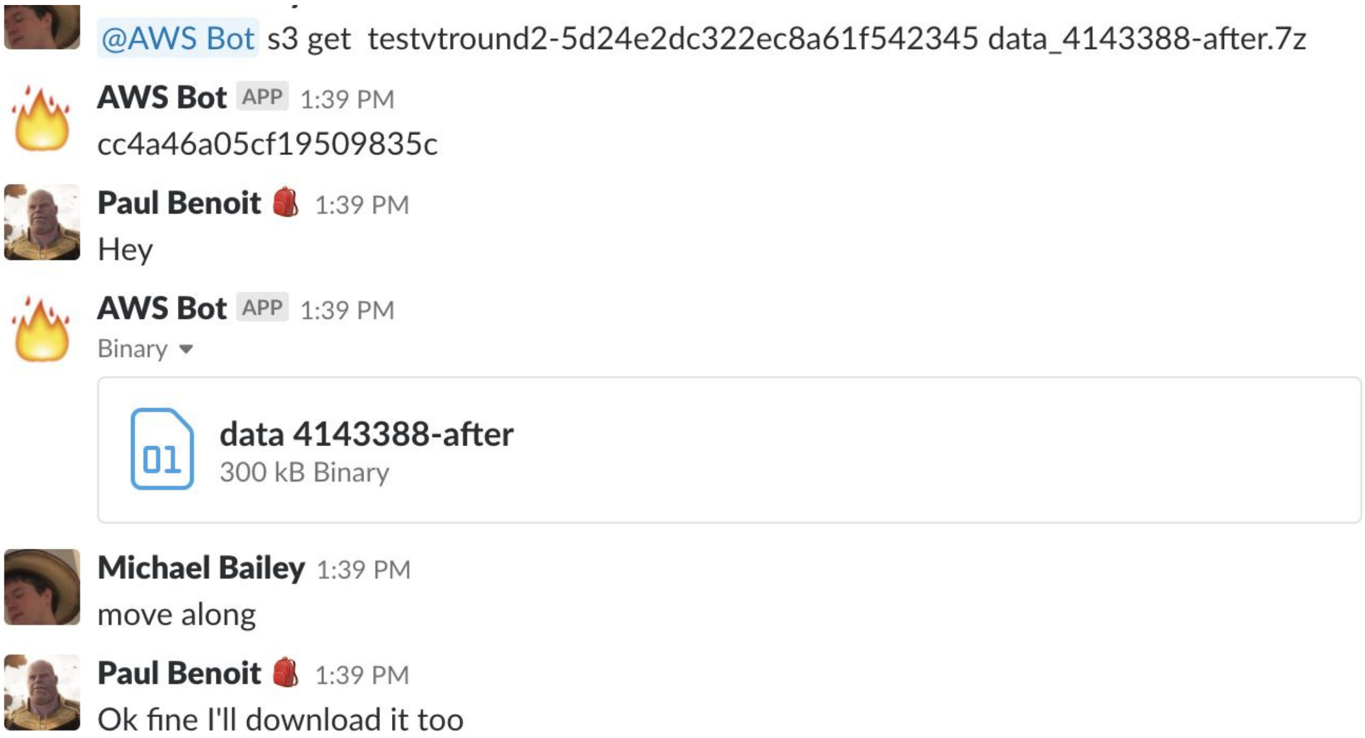
“Find evil”

Further collect

CTF Case Study

- UMD CTF
- Large number of event logs (evtx)
- Pain to read (not plaintext)
- Need to find the “odd pattern out”
  - Or, need to find a certain IP in certain questions, etc
    - This process is even better for multiple questions

CTF Case Study



@AWS Bot s3 get testvtround2-5d24e2dc322ec8a61f542345 data_4143388-after.7z

AWS Bot APP 1:39 PM
cc4a46a05cf19509835c

Paul Benoit 🎒 1:39 PM
Hey

AWS Bot APP 1:39 PM
Binary ▾

data 4143388-after
300 kB Binary

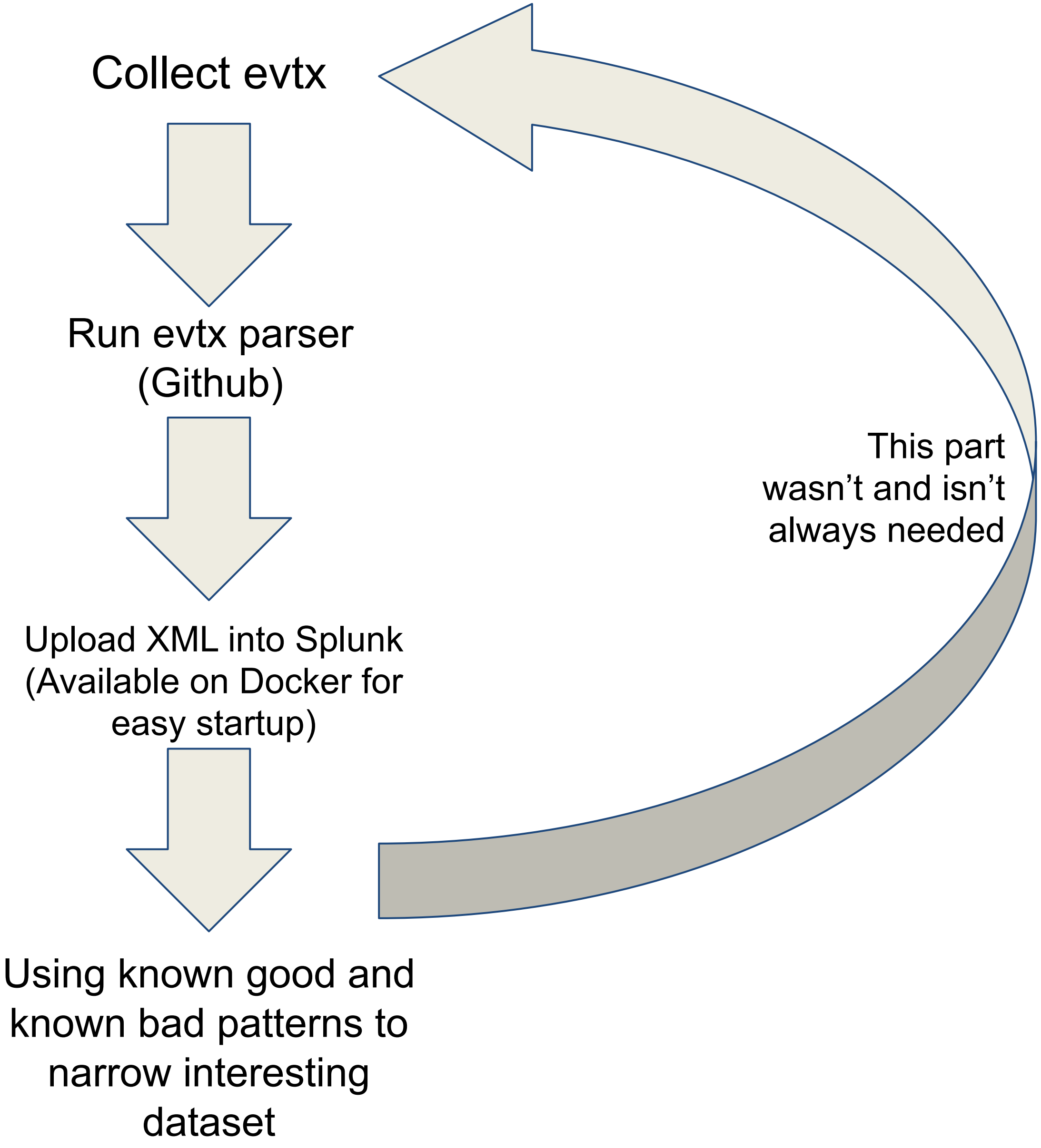
Michael Bailey 1:39 PM
move along

Paul Benoit 🎒 1:39 PM
Ok fine I'll download it too

Real Case Study

- Client opens RDP to the internet
- Attacker gets in, drops ransomware
- Ransomware propagates over SMB
- Crypsis gets LR data from affected system
- Increases scope until p0
- Identifies root cause from p0
- Gives recommendations based on p0

Case Study Process



Collect evtx

Run evtx parser (Github)

Upload XML into Splunk (Available on Docker for easy startup)

Using known good and known bad patterns to narrow interesting dataset

This part wasn’t and isn’t always needed

What’s an IoC?

- Indicator of compromise
  - High fidelity/confidence activity regarding compromise
- Commonly located via:
  - Pattern matching
    - Suspicious traffic
  - Keyword matching
  - Regex matching

Threat Intel

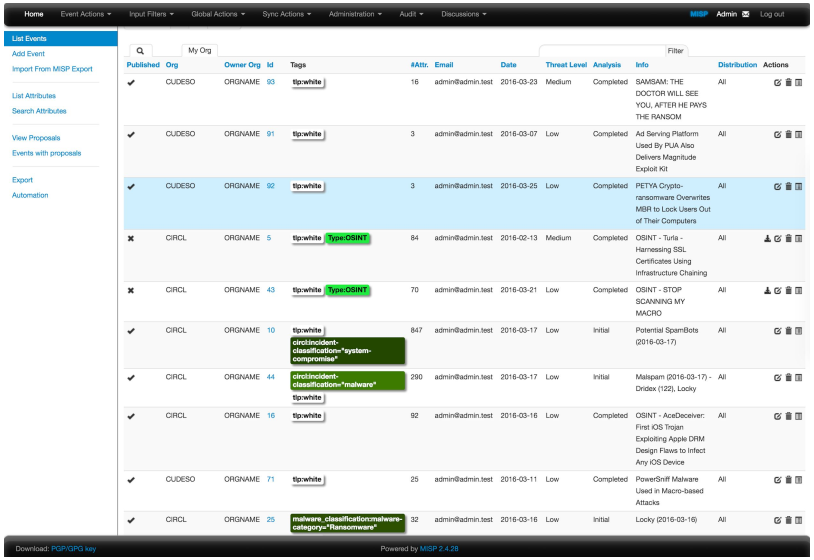
- Threat Intelligence
  - Like gold nowadays
  - Knowledge related to threats, what you'd expect
  - Tends to be inclusive to indicators
- MITRE Att&ck
  - Adversarial Tactics, Techniques, and Common Knowledge
  - Knowledge base of absolute **gold** covering threats, including a ton of APTs
  - API queryable

Where’s the Threat Intel?

- Research
  - So much of it is public, just very granular
- Past Work
  - Collected indicators from past work
- Bought out APIs
  - Extra popular

Private Offerings

- MISP

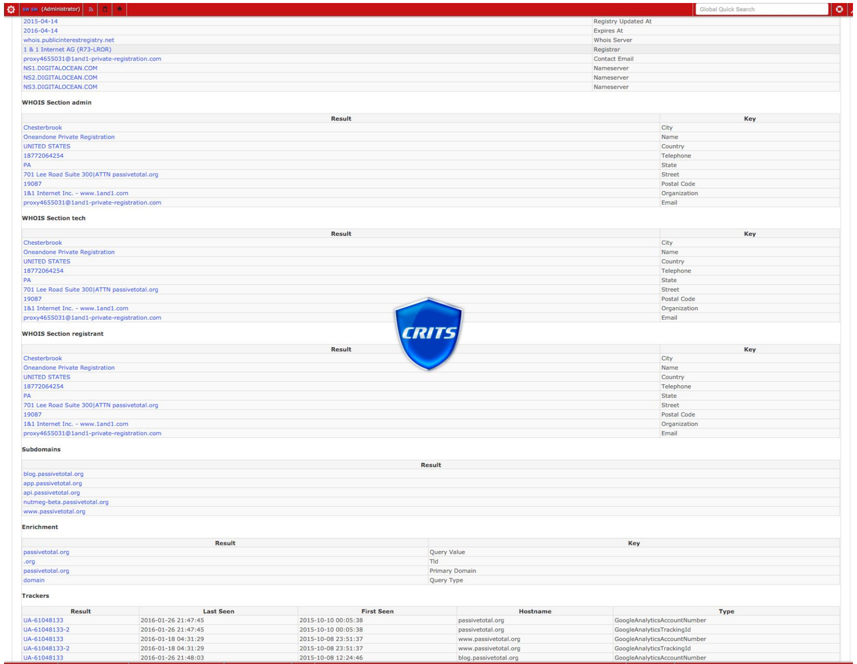


Published	Org	Owner Org	Id	Tags	#Attr.	Email	Date	Threat Level	Analysis	Info	Distribution	Actions
✓	CUDESO	ORGNAME	93	tlp:white	16	admin@admin.test	2016-03-23	Medium	Completed	SAMSAM: THE DOCTOR WILL SEE YOU, AFTER HE PAYS THE RANSOM	All	
✓	CUDESO	ORGNAME	91	tlp:white	3	admin@admin.test	2016-03-07	Low	Completed	Ad Serving Platform Used By PUA Also Delivers Magnitude Exploit Kit	All	
✓	CUDESO	ORGNAME	92	tlp:white	3	admin@admin.test	2016-03-25	Low	Completed	PETYA Crypto-ransomware Overwrites MBR to Lock Users Out of Their Computers	All	
✖	CIRCL	ORGNAME	5	tlp:white Type:OSINT	84	admin@admin.test	2016-02-13	Medium	Completed	OSINT - Turla - Harnessing SSL Certificates Using Infrastructure Chaining	All	
✖	CIRCL	ORGNAME	43	tlp:white Type:OSINT	70	admin@admin.test	2016-03-21	Low	Completed	OSINT - STOP SCANNING MY MACRO	All	
✓	CIRCL	ORGNAME	10	tlp:white circl:incident-classification="system-compromise"	847	admin@admin.test	2016-03-17	Low	Initial	Potential SpamBots (2016-03-17)	All	
✓	CIRCL	ORGNAME	44	circl:incident-classification="malware" tlp:white	290	admin@admin.test	2016-03-17	Low	Initial	Malspam (2016-03-17) - Dridex (122), Locky	All	
✓	CIRCL	ORGNAME	16	tlp:white	92	admin@admin.test	2016-03-16	Low	Completed	OSINT - AceDeceiver: First iOS Trojan Exploiting Apple DRM Design Flaws to Infect Any iOS Device	All	
✓	CUDESO	ORGNAME	71	tlp:white	25	admin@admin.test	2016-03-11	Low	Completed	PowerSniff Malware Used in Macro-based Attacks	All	
✓	CIRCL	ORGNAME	25	malware_classification:malware-category="Ransomware"	32	admin@admin.test	2016-03-16	Low	Initial	Locky (2016-03-16)	All	

Download: PGP/GPG key

Powered by MISP 2.4.28

- CRITS
  - Ya boy contributed



2015-04-14	Registry Updated At
2016-04-14	Expires At
whois.publicinterestregistry.net	Whois Server
1 & 1 Internet AG (R73-LROR)	Registrar
proxy4655031@1and1-private-registration.com	Contact Email
NS1.DIGITALOCEAN.COM	Nameserver
NS2.DIGITALOCEAN.COM	Nameserver
NS3.DIGITALOCEAN.COM	Nameserver

WHOIS Section admin

Result	Key
Chesterbrook	City
Oneandone Private Registration	Name
UNITED STATES	Country
18772064254	Telephone
PA	State
701 Lee Road Suite 300|ATTN passivetotal.org	Street
19087	Postal Code
1&1 Internet Inc. - www.1and1.com	Organization
proxy4655031@1and1-private-registration.com	Email

WHOIS Section tech

Result	Key
Chesterbrook	City
Oneandone Private Registration	Name
UNITED STATES	Country
18772064254	Telephone
PA	State
701 Lee Road Suite 300|ATTN passivetotal.org	Street
19087	Postal Code
1&1 Internet Inc. - www.1and1.com	Organization
proxy4655031@1and1-private-registration.com	Email

WHOIS Section registrant

Result	Key
Chesterbrook	City
Oneandone Private Registration	Name
UNITED STATES	Country
18772064254	Telephone
PA	State
701 Lee Road Suite 300|ATTN passivetotal.org	Street
19087	Postal Code
1&1 Internet Inc. - www.1and1.com	Organization
proxy4655031@1and1-private-registration.com	Email

Subdomains

Result
blog.passivetotal.org
app.passivetotal.org
api.passivetotal.org
nutmeg-beta.passivetotal.org
www.passivetotal.org

Enrichment

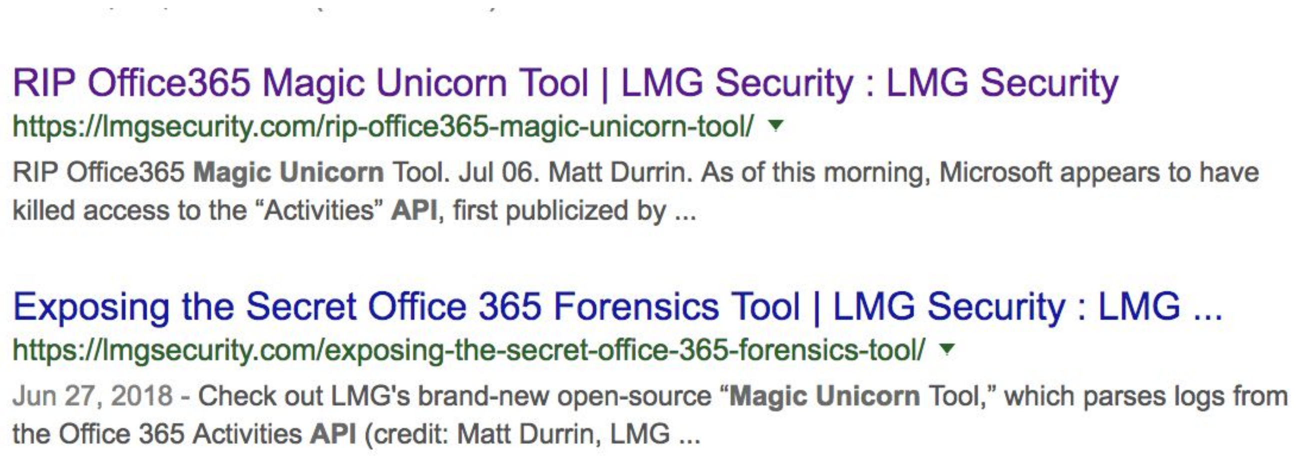
Result	Key
passivetotal.org	Query Value
.org	Tld
passivetotal.org	Primary Domain
domain	Query Type

Trackers

Result	Last Seen	First Seen	Hostname	Type
UA-61048133	2016-01-26 21:47:45	2015-10-10 00:05:38	passivetotal.org	GoogleAnalyticsAccountNumber
UA-61048133-2	2016-01-26 21:47:45	2015-10-10 00:05:38	passivetotal.org	GoogleAnalyticsTrackingId
UA-61048133	2016-01-18 04:31:29	2015-10-08 23:51:37	www.passivetotal.org	GoogleAnalyticsAccountNumber
UA-61048133-2	2016-01-18 04:31:29	2015-10-08 23:51:37	www.passivetotal.org	GoogleAnalyticsTrackingId
UA-61048133	2016-01-26 21:48:03	2015-10-08 12:24:46	blog.passivetotal.org	GoogleAnalyticsAccountNumber

About the Major Players

- Some are software companies
  - FireEye
  - Magnet
  - etc…
- Some share more than others
  - See: Magic Unicorn



RIP Office365 Magic Unicorn Tool | LMG Security : LMG Security
https://lmgsecurity.com/rip-office365-magic-unicorn-tool/ ▾
RIP Office365 **Magic Unicorn** Tool. Jul 06. Matt Durrin. As of this morning, Microsoft appears to have killed access to the “Activities” **API**, first publicized by ...

Exposing the Secret Office 365 Forensics Tool | LMG Security : LMG ...
https://lmgsecurity.com/exposing-the-secret-office-365-forensics-tool/ ▾
Jun 27, 2018 - Check out LMG's brand-new open-source “**Magic Unicorn** Tool,” which parses logs from the Office 365 Activities **API** (credit: Matt Durrin, LMG ...

Major Forensics Players

Questions?

- Some stuff can’t be disclosed related to work
- Ask anyways
- Ask me about work if you want
  - Give Crypsis their money’s worth

Qs

splunk.competitivecyber.club