nuix

Simple. Powerful. Precise.

Homebrew: Developing your own threat intel

Chris Brewer, Chris Woods

About Us

Chris Brewer

Senior Forensic Investigator

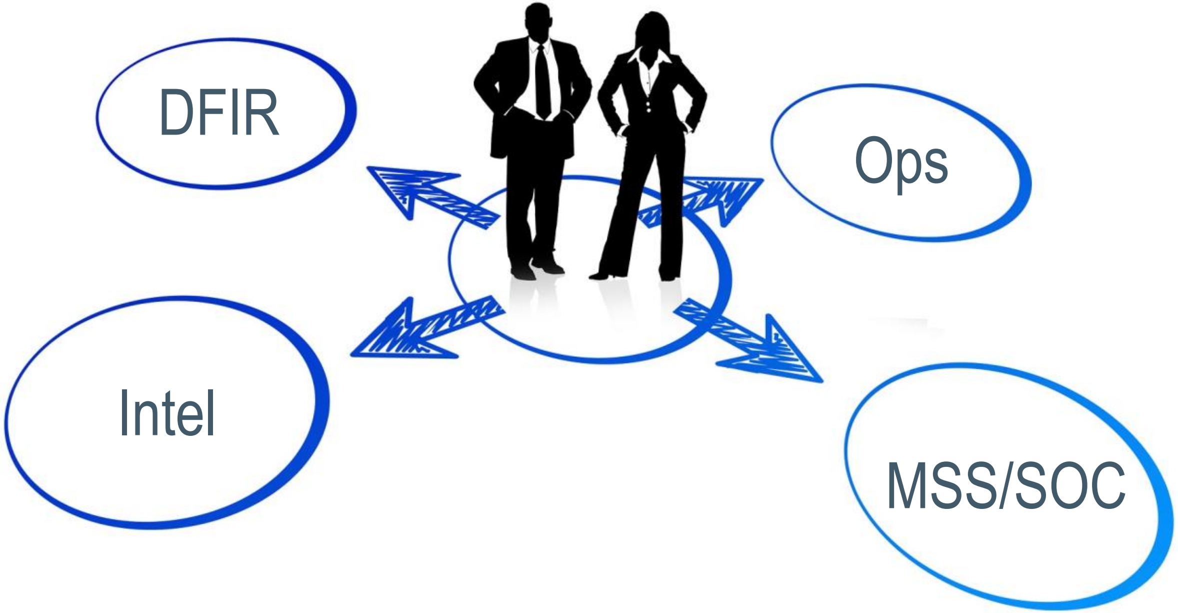
Chris Woods

Director of Audit & Compliance

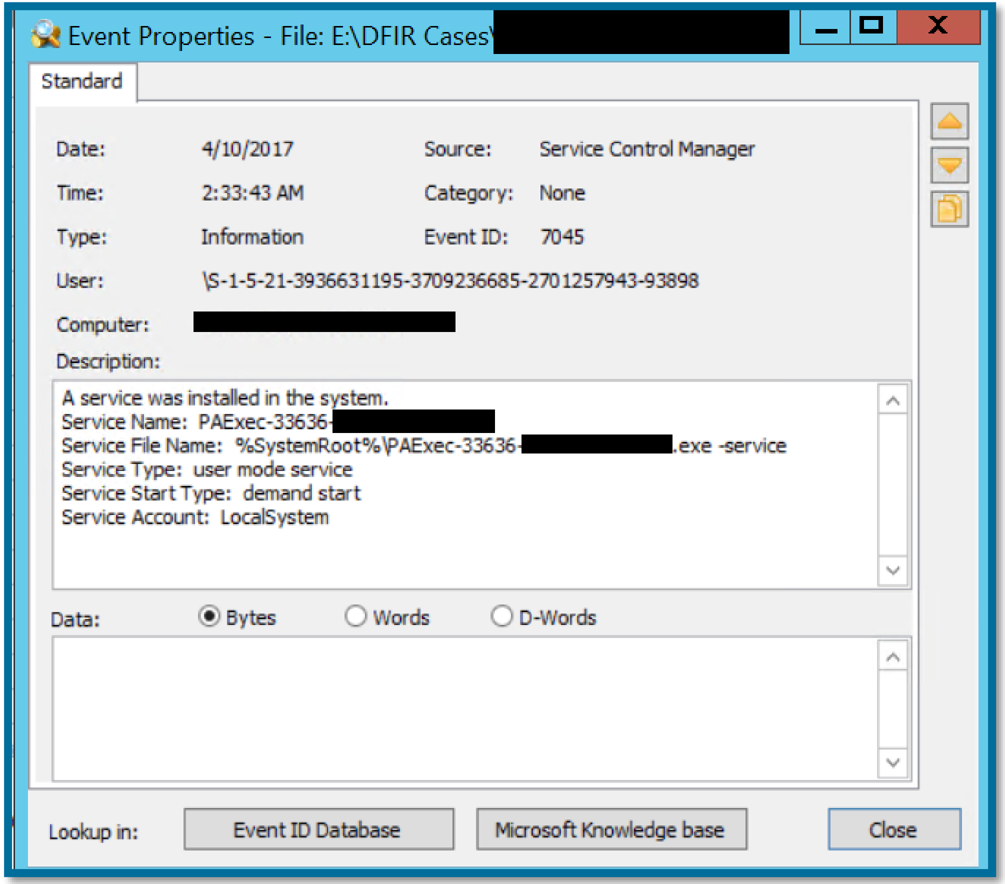
Threat Intelligence

What? Where? How?

Feedback Loop



Feedback Loop



Event Properties - File: E:\DFIR Cases\[redacted]

Standard

Date: 4/10/2017 Source: Service Control Manager

Time: 2:33:43 AM Category: None

Type: Information Event ID: 7045

User: \S-1-5-21-3936631195-3709236685-2701257943-93898

Computer: [redacted]

Description:

```
A service was installed in the system.
Service Name:  PAExec-33636-[redacted]
Service File Name:  %SystemRoot%\PAExec-33636-[redacted].exe -service
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem
```

Data: ● Bytes ○ Words ○ D-Words

Deployment

What data is valuable…

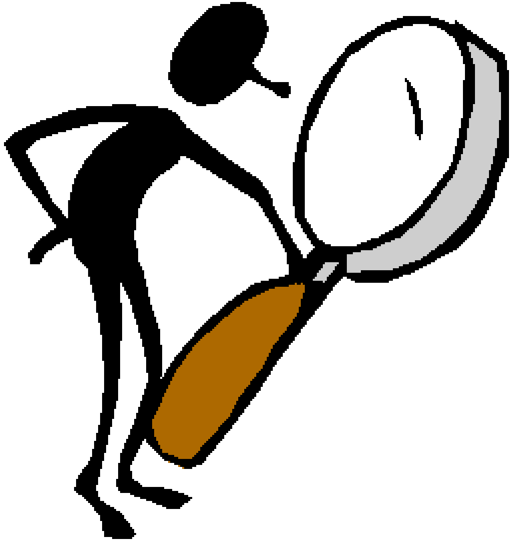
Where does it come from…

What are the use cases….

What do you use the data for….

What prevents you from using the data….

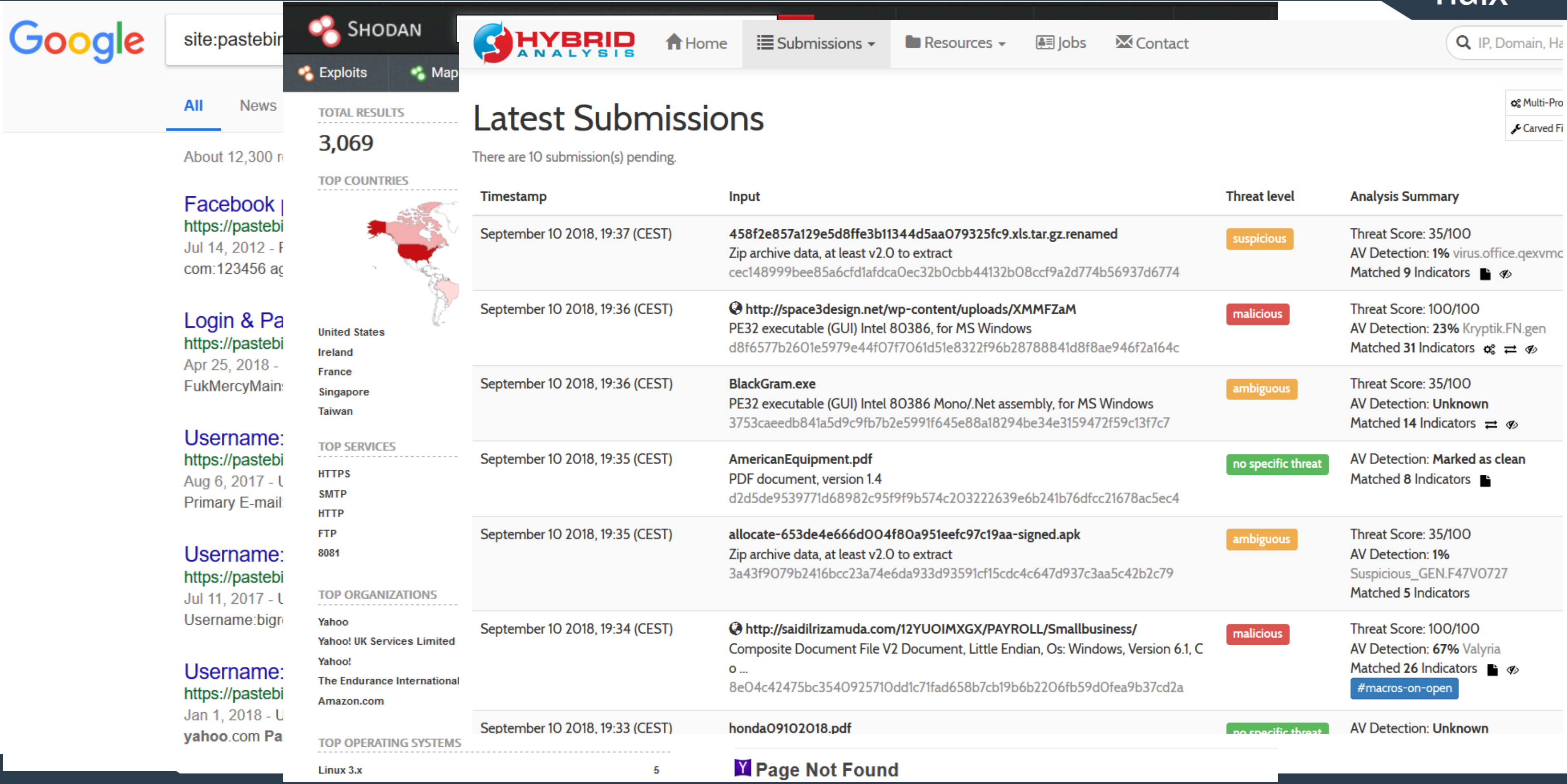
Formats



What does the intel “look like”?

- IOCs
- EDR rules
- Yara rules

OSINT Intel



About 12,300 r

Facebook |
https://pastebi
Jul 14, 2012 - F
com:123456 ag

Login & Pa
https://pastebi
Apr 25, 2018 -
FukMercyMain:

Username:
https://pastebi
Aug 6, 2017 - U
Primary E-mail:

Username:
https://pastebi
Jul 11, 2017 - U
Username:bigr

Username:
https://pastebi
Jan 1, 2018 - U
yahoo.com Pa

TOTAL RESULTS

3,069

TOP COUNTRIES

United States
Ireland
France
Singapore
Taiwan

TOP SERVICES

HTTPS
SMTP
HTTP
FTP
8081

TOP ORGANIZATIONS

Yahoo
Yahoo! UK Services Limited
Yahoo!
The Endurance International
Amazon.com

TOP OPERATING SYSTEMS

Linux 3.x	5

Latest Submissions

There are 10 submission(s) pending.

Timestamp	Input	Threat level	Analysis Summary
September 10 2018, 19:37 (CEST)	**458f2e857a129e5d8ffe3b11344d5aa079325fc9.xls.tar.gz.renamed** Zip archive data, at least v2.0 to extract cec148999bee85a6cfd1afdca0ec32b0cbb44132b08ccf9a2d774b56937d6774	suspicious	Threat Score: 35/100 AV Detection: **1%** virus.office.qexvmc Matched **9** Indicators
September 10 2018, 19:36 (CEST)	**http://space3design.net/wp-content/uploads/XMMFZaM** PE32 executable (GUI) Intel 80386, for MS Windows d8f6577b2601e5979e44f07f7061d51e8322f96b28788841d8f8ae946f2a164c	malicious	Threat Score: 100/100 AV Detection: **23%** Kryptik.FN.gen Matched **31** Indicators
September 10 2018, 19:36 (CEST)	**BlackGram.exe** PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows 3753caeedb841a5d9c9fb7b2e5991f645e88a18294be34e3159472f59c13f7c7	ambiguous	Threat Score: 35/100 AV Detection: **Unknown** Matched **14** Indicators
September 10 2018, 19:35 (CEST)	**AmericanEquipment.pdf** PDF document, version 1.4 d2d5de9539771d68982c95f9f9b574c203222639e6b241b76dfcc21678ac5ec4	no specific threat	AV Detection: **Marked as clean** Matched **8** Indicators
September 10 2018, 19:35 (CEST)	**allocate-653de4e666d004f80a951eefc97c19aa-signed.apk** Zip archive data, at least v2.0 to extract 3a43f9079b2416bcc23a74e6da933d93591cf15cdc4c647d937c3aa5c42b2c79	ambiguous	Threat Score: 35/100 AV Detection: **1%** Suspicious_GEN.F47V0727 Matched **5** Indicators
September 10 2018, 19:34 (CEST)	**http://saidilrizamuda.com/12YUOIMXGX/PAYROLL/Smallbusiness/** Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, C o ... 8e04c42475bc3540925710dd1c71fad658b7cb19b6b2206fb59d0fea9b37cd2a	malicious	Threat Score: 100/100 AV Detection: **67%** Valyria Matched **26** Indicators #macros-on-open
September 10 2018, 19:33 (CEST)	**honda09102018.pdf**	no specific threat	AV Detection: **Unknown**

Page Not Found

Case Study 1 – Password Spraying

Company Background:

Construction and Engineering firm with offices world wide

What they did:

Correlating single source IP’s logging in to domain controllers using multiple user accounts. ~10 failed attempts within an hour

In their own words:

“… actually didn't give us nearly as bad of a FP count as we thought it would. This alert has caught nation states and pentesters a total of 4 times over the past year attempting to password spray while either internal or external”

Case Study 2 – Port Scanning

Company Background:

Large power company in the Southwestern United States

What they did:

Count of unique ports scanned by a single source bucketed by day averaged by a total amount over 7 days to create a % chance that it is a "new" port scan or if it's a continued automated scan.

In their own words:

“…caught multiple pentesters who either got in or tried to hit our external networks just watching this alert”

Case Study 3 - OSINT

Company Background:

Large financial company in the United States

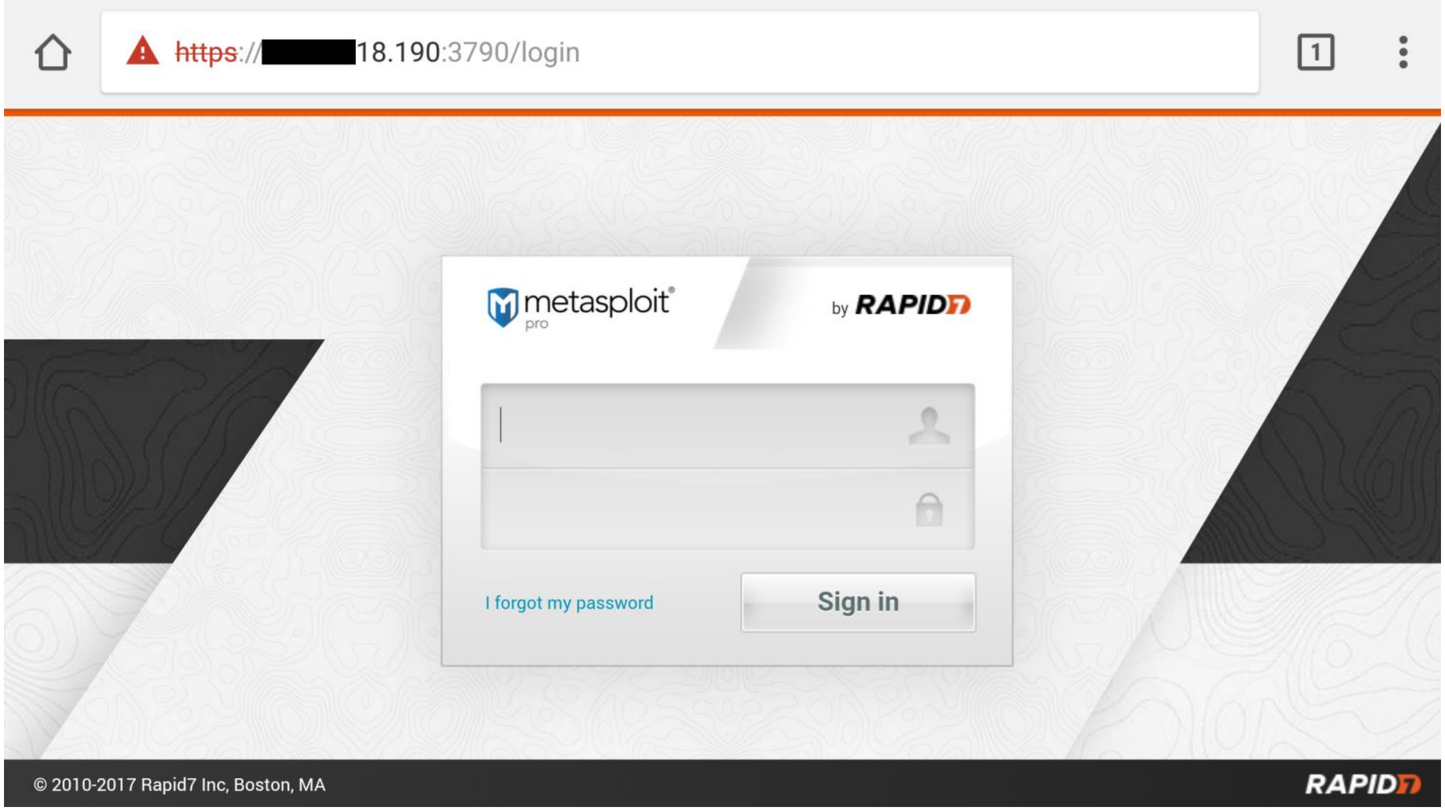
How it started:

Office 365 brute force

How it escalated:

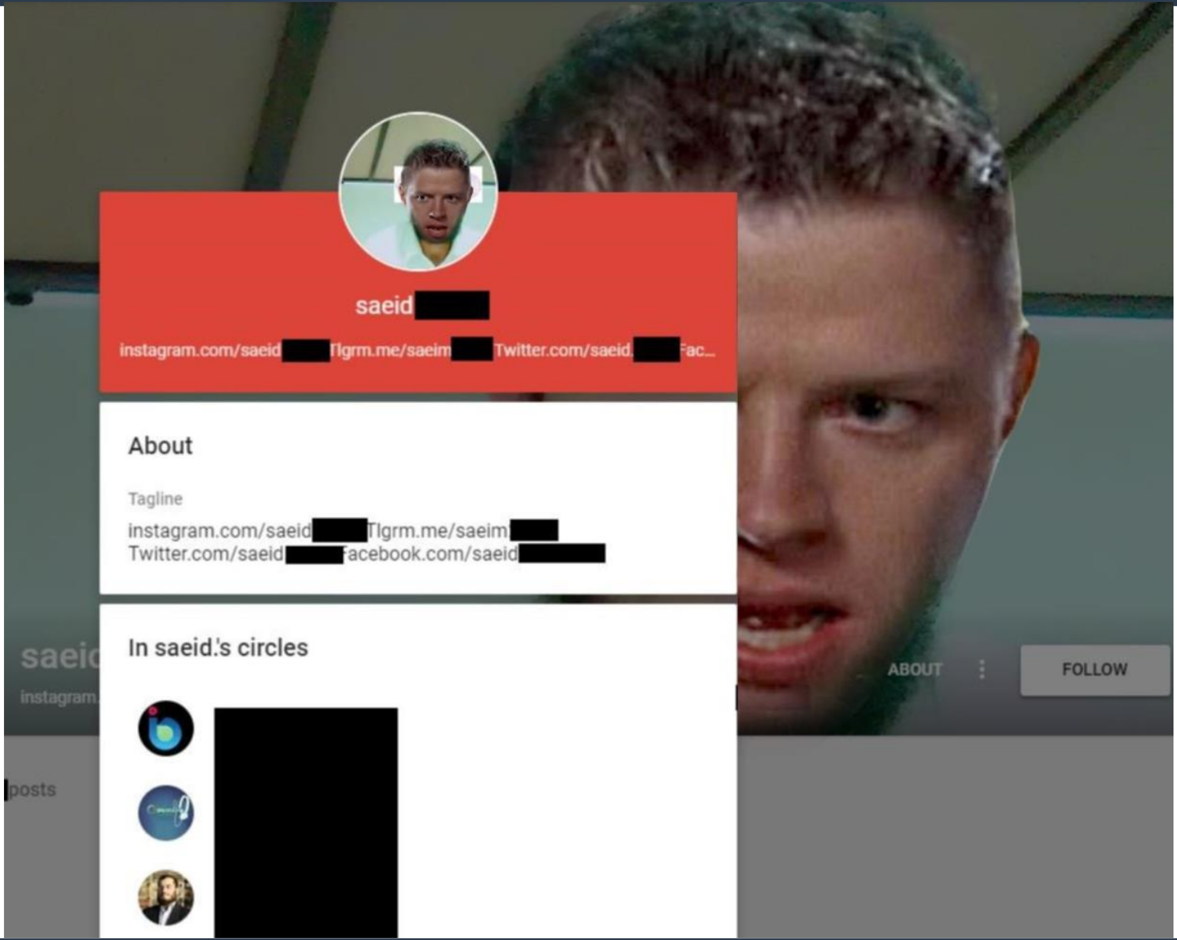
Statistical analysis of connections to Office 365 revealed abnormal connection from 3rd party IT contract company

Case Study 3 - OSINT



~~https~~://[redacted]18.190:3790/login

Case Study 3 - OSINT



saeid [redacted]

instagram.com/saeid[redacted]Tlgrm.me/saeim[redacted]Twitter.com/saeid.[redacted]Fac...

About

Tagline

instagram.com/saeid[redacted]Tlgrm.me/saeim[redacted]
Twitter.com/saeid[redacted]acebook.com/saeid[redacted]

In saeid.'s circles

[redacted]

Questions?

FIND OUT MORE:

- nuix.com
- nuix.com/blog
- twitter.com/nuix
- facebook.com/nuixsoftware
- linkedin.com/company/nuix
- youtube.com/nuixsoftware

nuix

Simple. Powerful. Precise.