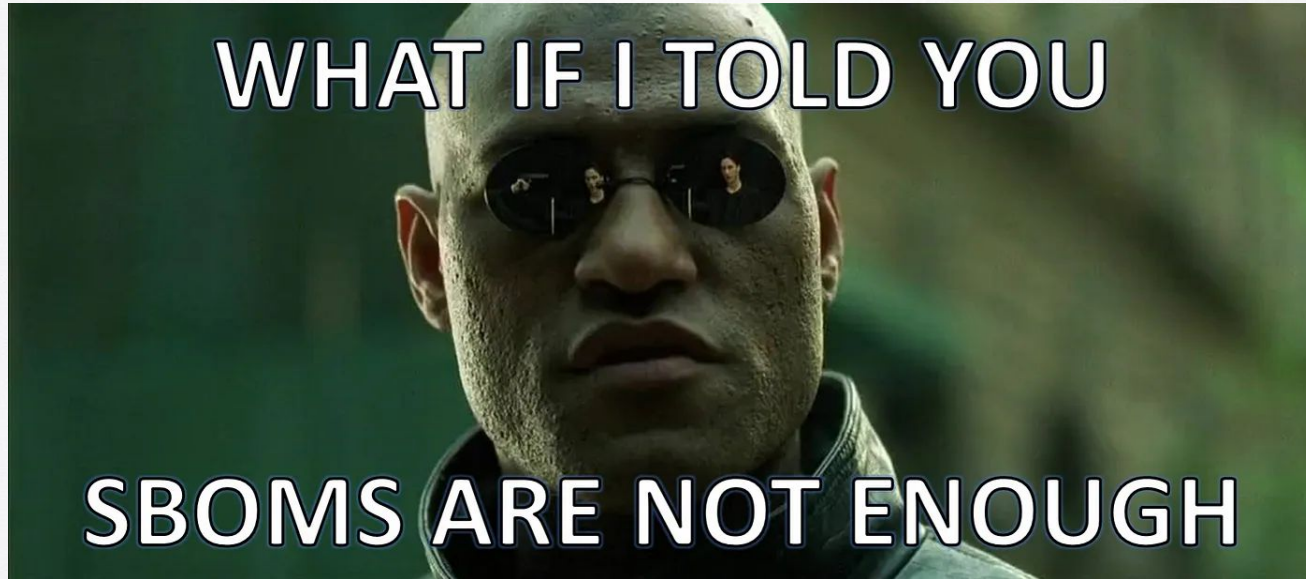


Software Bills of Behaviors: Why SBOMs aren't enough



Andrew Hendela
andrew@karambit.ai



KARAMBIT.AI

tl;dr

- There are a lot of software supply chain attacks
- SBOM doesn't solve for them
- Software Bills of Behaviors give control and understanding to your software supply chain

Should You Listen To Me?



Andrew Hendela
Co-Founder



Over a decade of R&D in
automating offensive
and defensive
cybersecurity problems

cyber attribution,
exploit development,
malware analysis,
vulnerability research

SolarWinds

- Russian-attributed targeted supply chain attack
 - 18,000 Orgs as customers
 - Handful of Orgs actually attacked
 - US Agencies, Some Fortune 500, Cyber Companies
 - All had to remediate in some way

SolarWinds is 'largest' cyberattack ever, Microsoft president says

The hack sent malware to about 18,000 public and private organizations.



Scope of Russian Hacking Becomes Clear: Multiple U.S. Agencies Were Hit

The Pentagon, intelligence agencies, nuclear labs and Fortune 500 companies use software that was found to have been compromised by Russian hackers. The sweep of stolen data is still being assessed.

3CX

- DPRK-attributed *Chain* supply chain attack
- Mandiant: 3CX was the *second* org compromised in the chain
- First supply chain compromise led into 3CX
- Seems opportunistic to get to crypto-companies

MANDIANT
NOW PART OF Google Cloud

Platform

Solutions

Intelligence

Services

Resources

Company

BLOG

3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible

PyTorch

December 31, 2022

Compromised PyTorch-nightly dependency chain
between December 25th and December 30th, 2022.



by The PyTorch Team

- **December 2022**
- **Python compiled dependency stole data**
- **Caught pretty quickly**
- **“Security Researcher”**
- **The bar is *low* for these attacks**

Tons of app store malware

- Happens all the time
- High level permission understanding, no understanding of what it does with them

**Android app breaking bad:
From legitimate screen
recording to file exfiltration
within a year**

ESET researchers discover AhRat – a new Android RAT based on AhMyth – that exfiltrates files and records audio

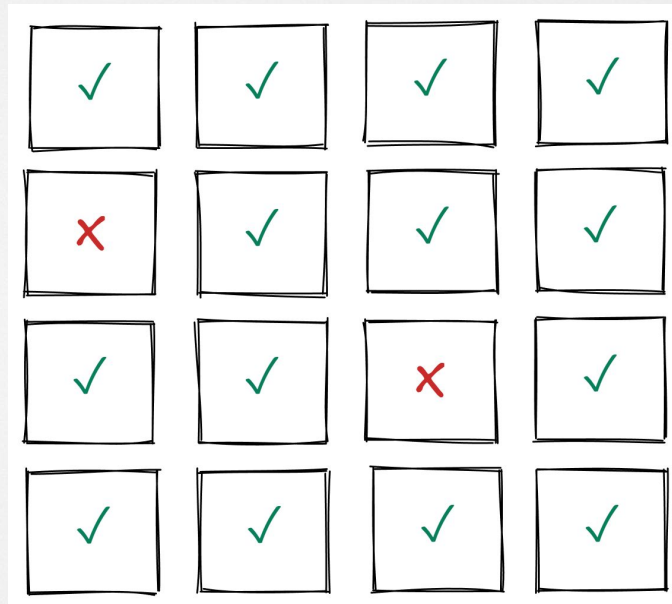
Trust me

“Supply chains, both physical and digital, have an explicit reliance on trust, and adversaries have taken notice.”

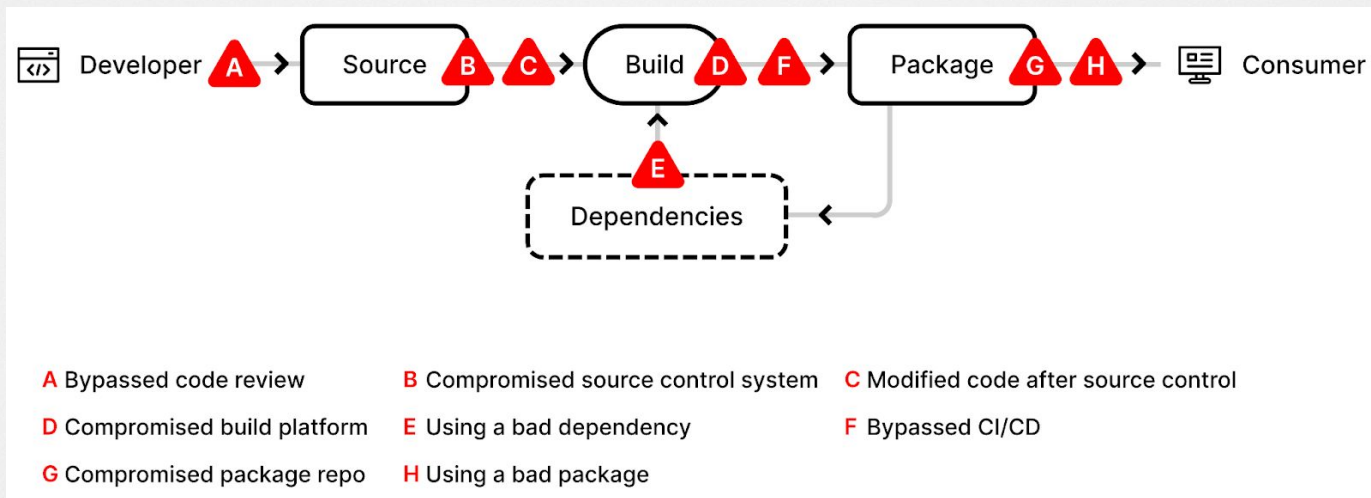
- [Microsoft Digital Defense Report 2021](#)

Trust Limitations

- Lack of *Information*
- Checkboxes and questionnaires
- Lots of software being pulled in
 - Libs, docker images, etc.

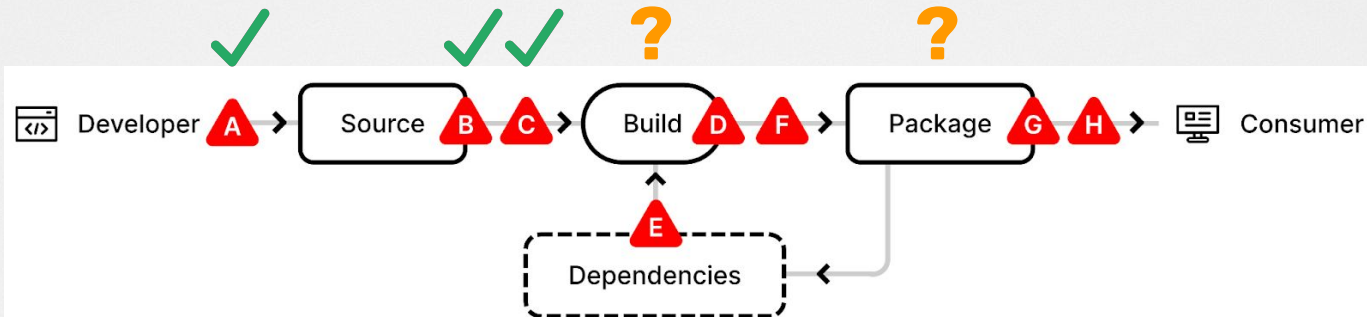


Supply Chain Integrity Attacks



Google's [Supply-chain Levels for Software Artifacts](#) (SLSA) framework

Supply Chain Integrity Attacks



- | | | |
|------------------------------|-------------------------------------|--------------------------------------|
| A Bypassed code review | B Compromised source control system | C Modified code after source control |
| D Compromised build platform | E Using a bad dependency | F Bypassed CI/CD |
| G Compromised package repo | H Using a bad package | |

- Heavy industry focus covering Source Integrity (A, B)
- Policy and signing post build (E, G, H)
- How do you address threats that bypass source?

Current Defensive Focus



**Software Bill of
Materials (SBOMs)**



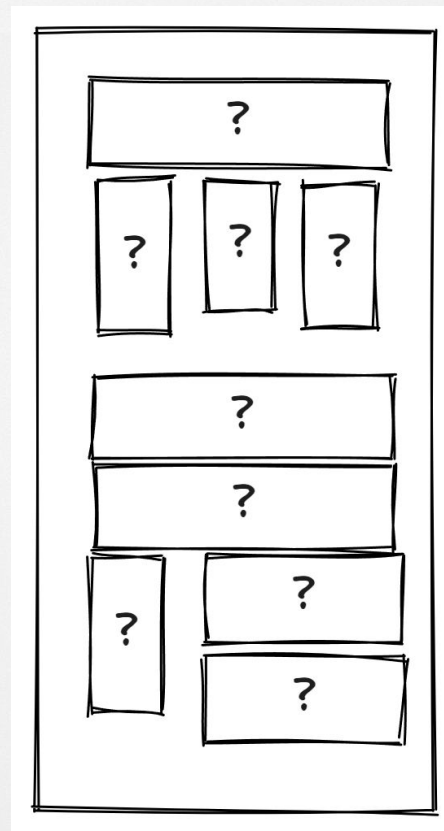
**Vulnerability
Detection/VEX**



**Post
Compromise
Analysis**

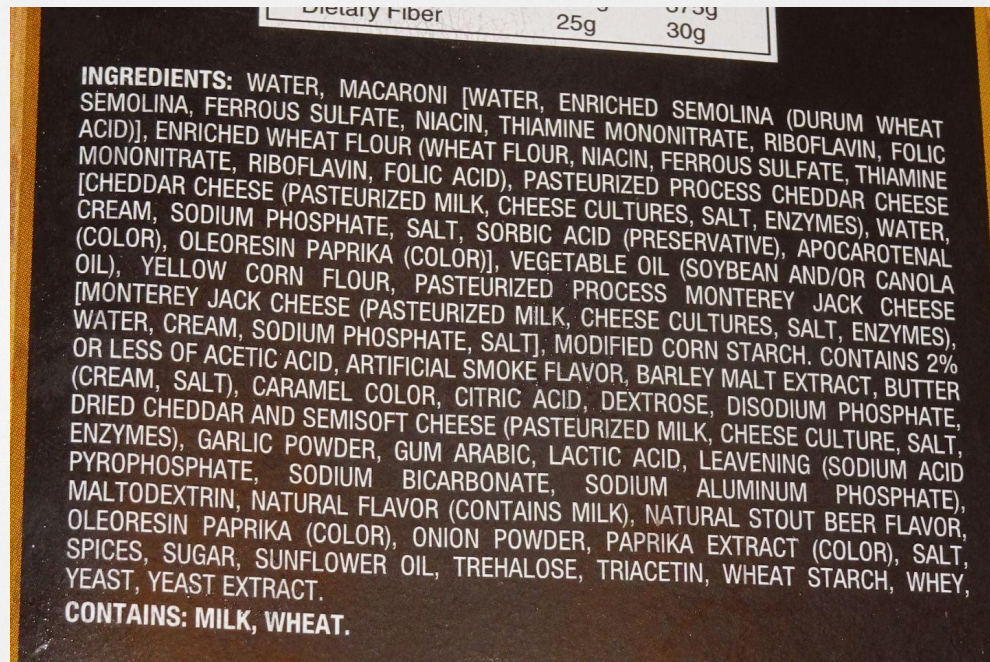
SBOMs: What they are

- Do we even know the components in our software?



SBOMs: Use cases

- Check a box?
- Read them?
- Vulns
- Known Bad



SBOMs: Limitations

- Doesn't tell you anything by itself
- Needs to be trustworthy
- Needs to be complete
- Again, trust
- Information

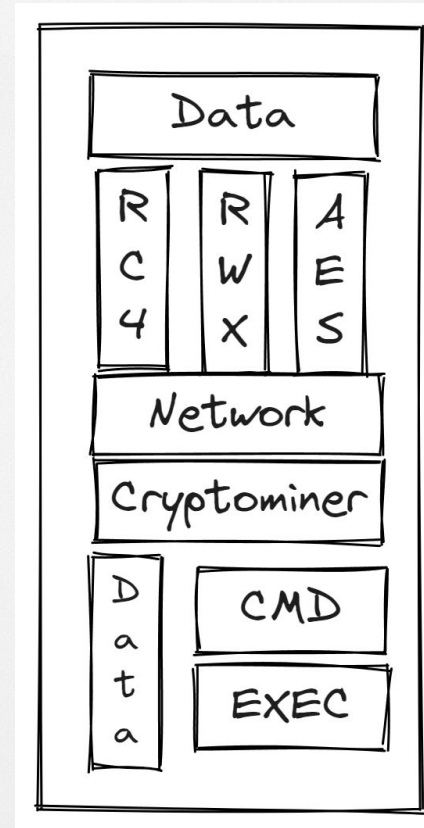
ENZYMES), GARLIC POWDER, GUM ARABIC, LACTIC ACID, LEAVENING (SODIUM ACID PYROPHOSPHATE, SODIUM BICARBONATE, SODIUM ALUMINUM PHOSPHATE), MALTODEXTRIN, NATURAL FLAVOR (CONTAINS MILK), NATURAL STOUT BEER FLAVOR, OLEORESIN PAPRIKA (COLOR), ONION POWDER, PAPRIKA EXTRACT (COLOR), SALT, SPICES, SUGAR, SUNFLOWER OIL, TREHALOSE, TRIACETIN, WHEAT STARCH, WHEY, YEAST, YEAST EXTRACT.
CONTAINS: MILK, WHEAT.

SBOMs: What they don't answer

- Should I trust this?
- What will software actually do?

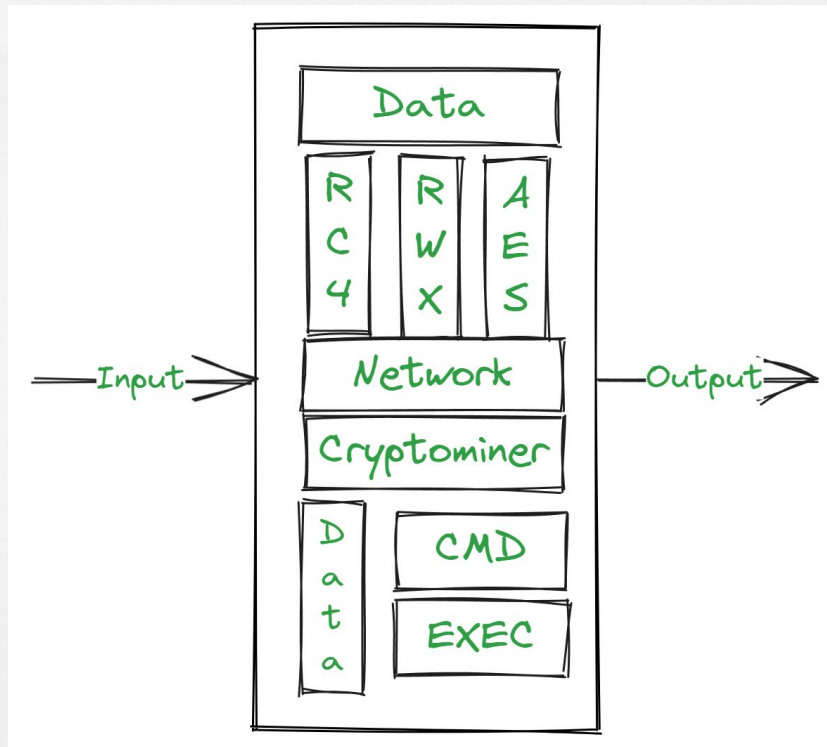
Software Bill of Behaviors

- *Closer* to information
- Make informed decisions
 - Do you want your AV mining crypto?
 - What will this app do with my data?



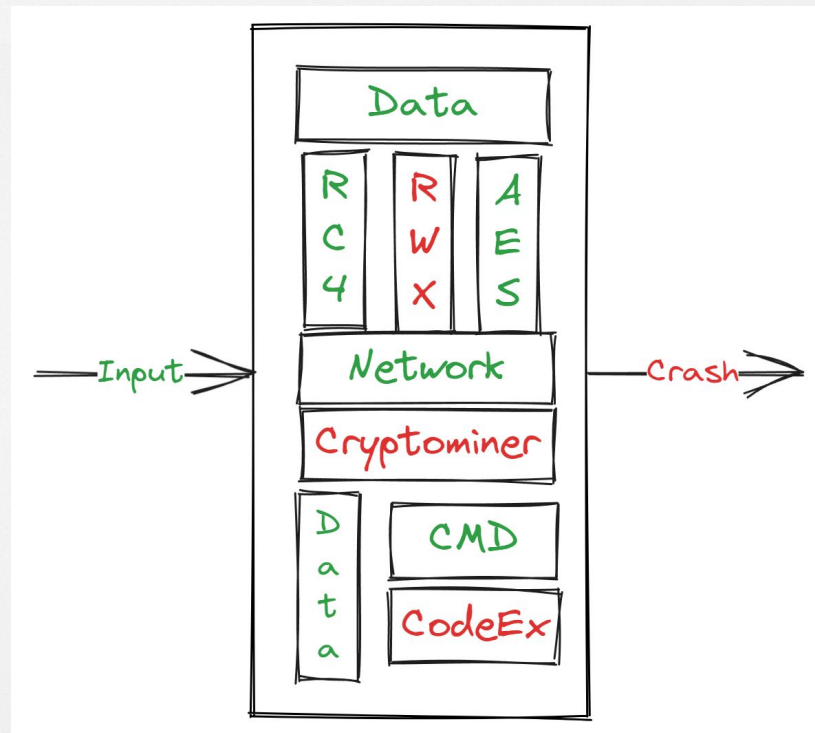
What is a Behavior?

- **Intended Actions**
 - Inputs and outputs
 - Data use, network connections, ATT&CK-y things
 - Algorithms, data structures, math



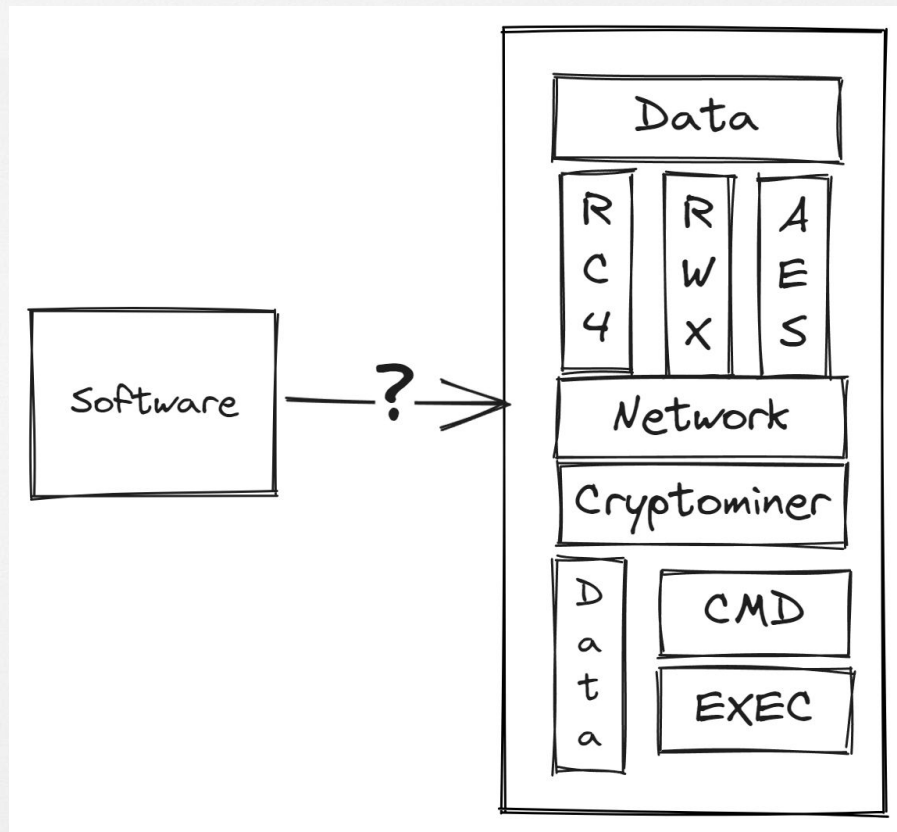
What is a Behavior?

- Unintended Actions
 - Data use, network connections, ATT&CK-y things
 - Crashes
 - Exploits



Getting a Software Bill of Behaviors

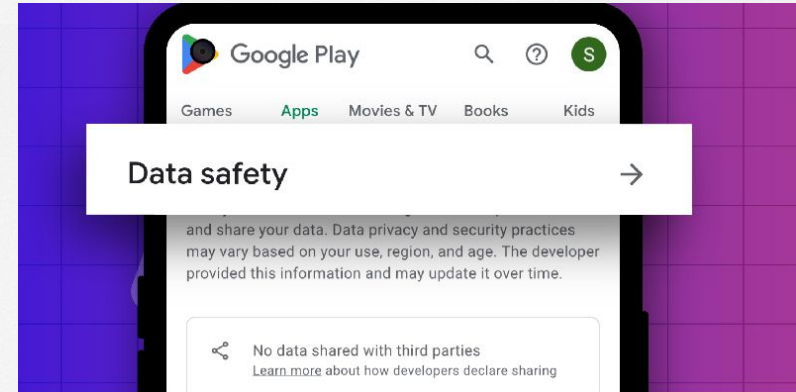
- Ask a vendor politely
 - Domains/IPs
 - Patch notes
- Build it from source
- Build it from binaries
- Detonation chamber/Sandboxes



So What?

Behavior Understanding

- Everyone is using software that they don't understand
 - Libraries, Docker Images, Windows, Phone Apps
- “80% of Apps” - Mozilla



Mozilla Study: Data Privacy Labels for Most Top Apps in Google Play Store are False or Misleading



By Mozilla | Feb. 23, 2023

Tracking

Opinion | **THE PRIVACY PROJECT**

Smartphones Are Spies. Here's Whom They Report To.

By Stuart A. Thompson and Charlie Warzel Dec. 20, 2019

“Companies often pay the apps for access, doling out as much as \$20 per 1,000 unique users each month or as little as \$2 per 1,000”

Crypto Mining



Krebs on Security
In-depth security news and investigation

HOME ABOUT THE AUTHOR ADVERTISING/SPEAKING

Norton 360 Now Comes With a Cryptominer

January 6, 2022

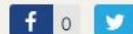
You can now mine cryptocurrency with your antivirus software. Wait, what?

By [Paul Lilly](#) published June 04, 2021

Norton 360 antivirus is getting a built-in Ethereum mining tool.

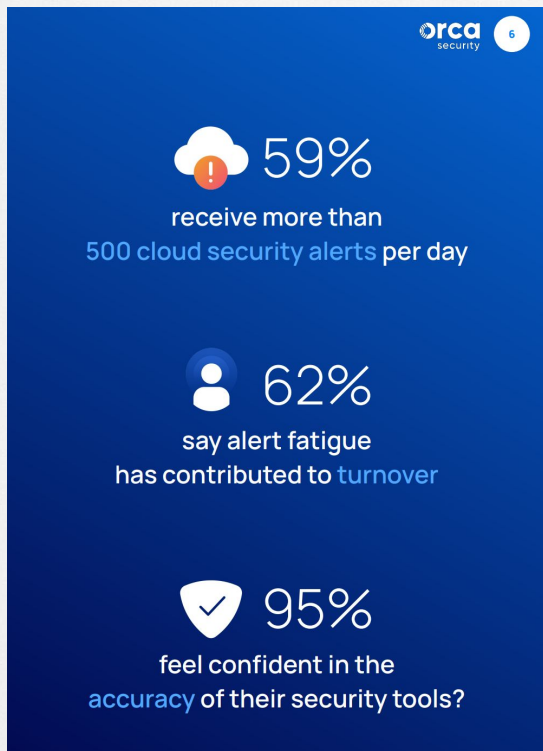
FAQ: Norton Crypto

Posted: 20-Jul-2021 | 11:38AM - Edited: 15-Mar-2022 | 11:39PM -



The below FAQ could address some of your questions.

Behavior Validation



- Alert Fatigue
- Tool tuning

What is it?

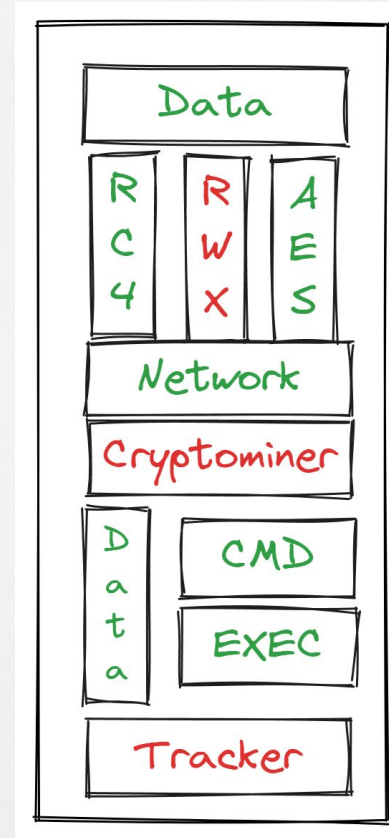
create reverse shell

[ATT&CK]: Execution::Command and Scripting Interpreter::Windows Command Shell [T1059.003]

[MBC]: Impact::Remote Access::Reverse Shell [B0022.001]

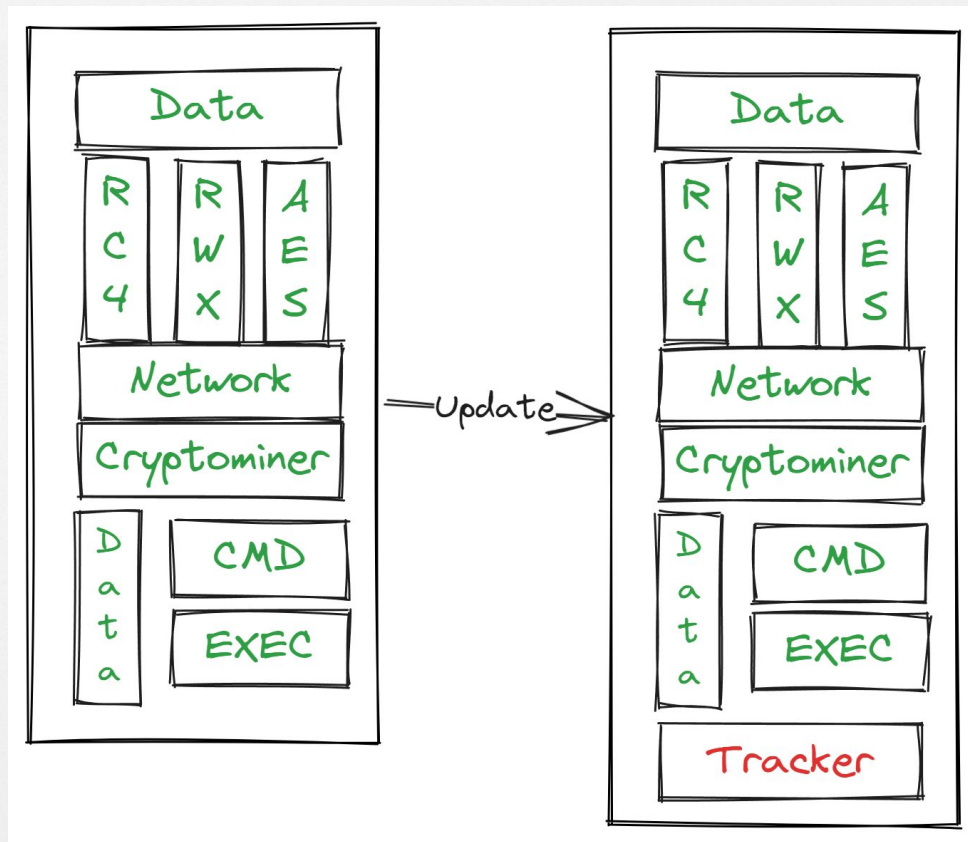
Unexpected Behaviors

- Unintended behaviors
- Inserted behaviors
- Exploits
- Arbitrary code execution



Changes Between Updates

- Find apps adding behaviors
- Know what updates change



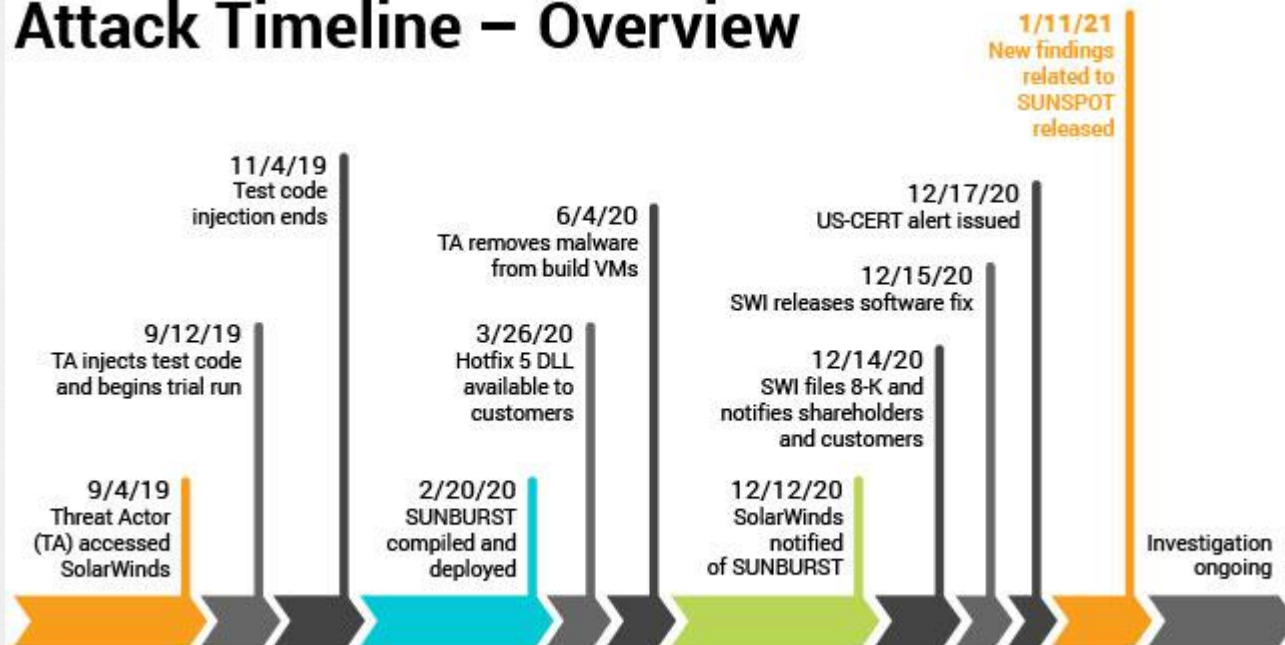
AhRat

**Android app breaking bad:
From legitimate screen
recording to file exfiltration
within a year**

ESET researchers discover AhRat – a new Android RAT based on AhMyth – that exfiltrates files and records audio

SolarWinds

Attack Timeline – Overview



All events, dates, and times approximate and subject to change; pending completed investigation.

3CX

allocate RWX memory

[MBC]: Memory::Allocate Memory [C0007]



encrypt data using RC4 KSA

[ATT&CK]: Defense Evasion::Obfuscated Files or Information [T1027]

[MBC]: Cryptography::Encrypt Data::RC4 [C0027.009]

[MBC]: Cryptography::Encryption Key::RC4 KSA [C0028.002]



**Unobfuscated behavioral changed indicated
encrypted payload, decrypted payload
connected to C2: none of this intended by the
developer**

Too Afraid to Patch Your Stuff



National Cyber
Security Centre

The problems with patching

Applying patches may be a basic security principle, but that doesn't mean it's always easy to do in practice.

“Patching takes time, and costs money. ... Patching introduces risk.” - NCSC

“Mean Time to Remediation (MTTR) for Critical Severity vulnerabilities is 65 days” - Edgescan

Patch Tuesday

3.6K

unique updated
/Windows binaries
(.dll/.exe/.sys)

28.7K

hours to manually
reverse engineer
each month

90%

Software with
minimal changes to
behaviors

Vulnerable Function Use

- **OpenSSL**
- **Log4shell**
- **Named Vuln of the Month**

Vulnerable Function Use

```

*****
*                               FUNCTION                               ...
*****
int __stdcall X509_VERIFY_PARAM_add0_policy(X509_VERIFY...

int          EAX:4          <RETURN>
X509_VERIFY_PA...  RDI:8          param
ASN1_OBJECT *    RSI:8          policy
undefined8      Stack[-0x10]... local_10          XREF[2]:    004d1d1c (W),
                                                    004d1d33 (R)
undefined8      Stack[-0x18]... local_18          XREF[2]:    004d1d18 (*),
                                                    004d1d26 (*)
X509_VERIFY_PARAM_add0_policy          XREF[3]:    Entry Point (*), 005aa44c,
                                                    005cf5f8 (*)


```


Location	Label	Code Unit	Ref Type
	Entry Point	??	EXTERNAL
005aa44c		fde_table_entry	INDIRECTION
005cf5f8		ddw X509_VERIFY_PA...	DATA


Malware Analysis

Process and service actions ⓘ

Processes Tree

 3980 - 'C:\Users\user\Desktop\2022-03-18-kpatched-notepad.exe'

 ↳ 4576 - 'C:\Windows\System32\calc.exe'

 6976 - C:\Windows\System32\OpenWith.exe C:\Windows\system32\OpenWith.exe -Embedding

Synchronization mechanisms & Signals ⓘ

Mutexes Created

Takeaways

- **SBOM Limitations**
- **SBOB benefits/Use Cases**
- **Software Developers Should know (they don't)**

Questions?

Andrew Hendela

andrew@karambit.ai

<https://karambit.ai>

www.linkedin.com/in/andrew-hendela