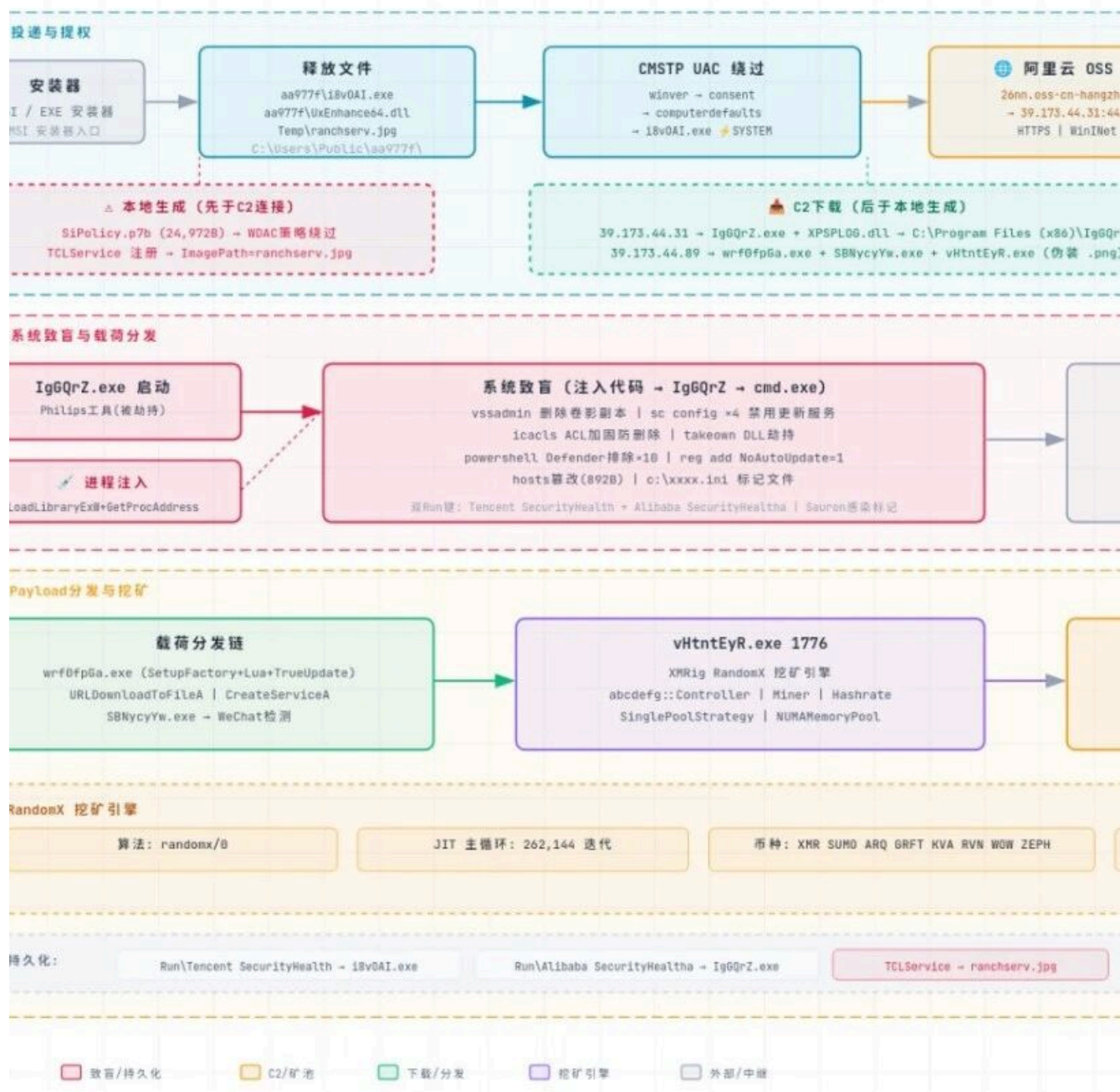


「SEID实战共享」借壳、致盲、挖矿：针对多层C2架构的银狐黑产剖析

mp.weixin.qq.com/s/OWOCPhn9Sq94Oj7P4F82Y1A

CACT



「本次分析的全部素材均来自 SEID 社区成员的主动提交与共享，感谢中煤集团、中国中化、哈电集团等企业提供的信息」

近期，国资国企网络威胁信息共建共享平台（SEID）陆续收到多家央企成员单位上报的同类可疑样本。经关联分析与逆向研判，确认这是一起自今年第二季度起持续活跃的大规模银狐远控+挖矿组合攻击。攻击者批量仿冒常见软件安装包（MSI/EXE），捆绑传播 Gh0stRAT 变种及基于 XMRig 的挖矿程序，技术层面融合了 BYOVD 致盲、WDAC 策略伪造、阿里云 OSS 投递、三层 C2 架构、无文件内存注入等高级攻防手法，驻留持久化设计极为缜密，清除难度极高。

现将本次攻击的完整剖析向公众披露，以供更广泛的国资国企安全团队参考布防。

1

样本整体流程

样本整体执行流程可按功能划分为三个阶段：第一阶段（蓝色）为初始感染阶段，主要完成样本解包，并从远端服务器拉取后续阶段所需的恶意文件及EDR致盲组件；第二阶段（粉色）为致盲与驻留阶段，利用获取的致盲组件禁用EDR防护，随后解密Gh0stRAT Payload并以无文件落地的方式实现内存驻留；第三阶段（黄色）为挖矿执行阶段，启动挖矿程序开始恶意挖矿操作。详细流程见图1：

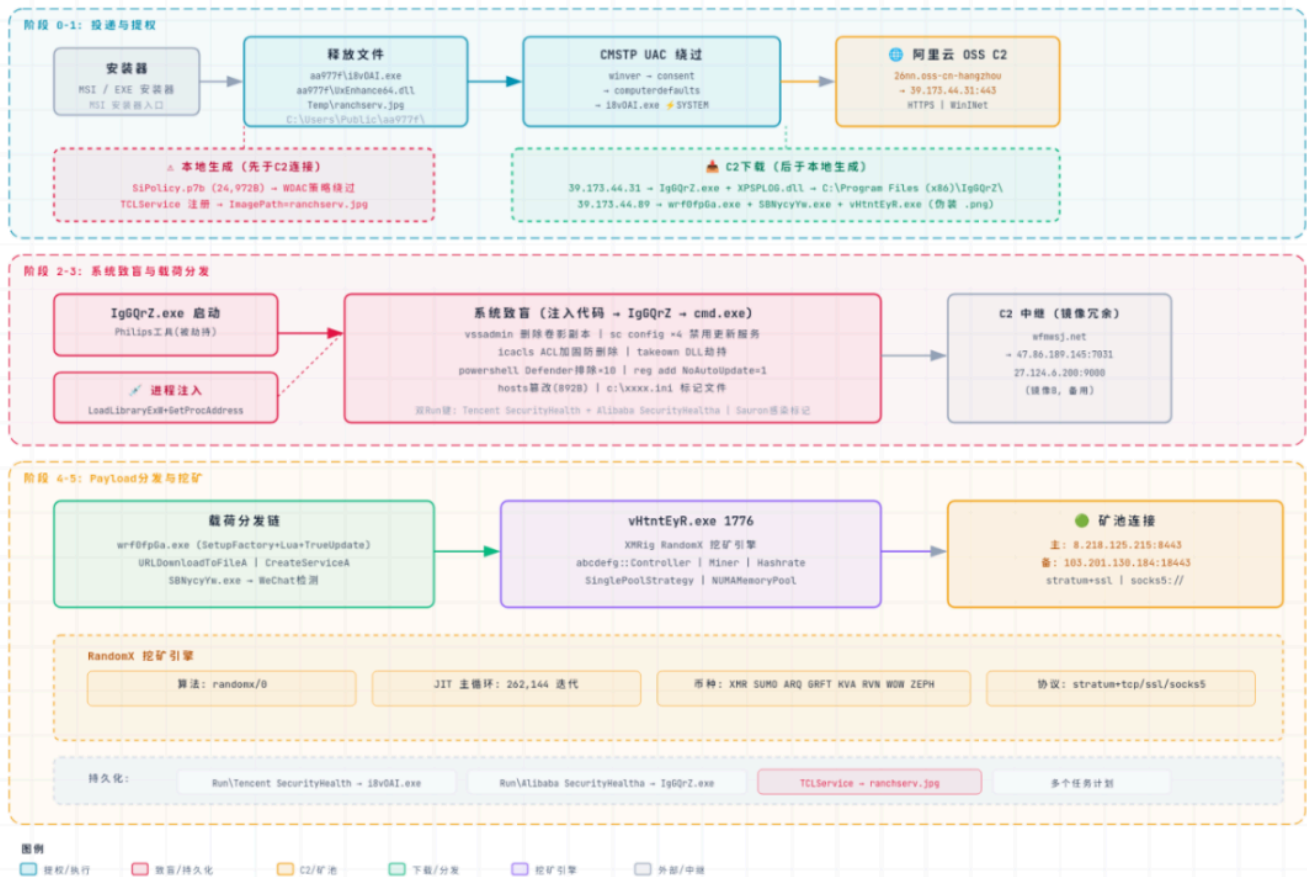


图 1 整体攻击流程

2

细节分析及特征披露

(一) 初始阶段

在初始感染阶段，攻击者通过仿造MSI或EXE格式的日语环境常见应用程序，如：NumLockLock、PpcNotif.Provider.RequiredApp（松下相关应用）及少部分国产大模型相关程序，如：豆包等，诱使相关应用程序使用者安装伪造的应用程序，进而实现传播Gh0stRAT及挖矿程序的目的。

(二) 感染阶段（投递&提权）

运行初始样本后，其将后续核心恶意组件释放至 C:\Users\Public\{random char} 及 C:\Windows\Temp 目录下，主要包括：具备 UAC Bypass 能力的第二阶段“白+黑”组合样本、

伪装为 .jpg 图片的 TrueSight V2.0.2 内核驱动（ranchserv.jpg）以及 WDAC 策略文件（SiPolicy.p7b），为后续禁用安全工具、BYOVD 致盲及多层持久化部署做好充分准备。

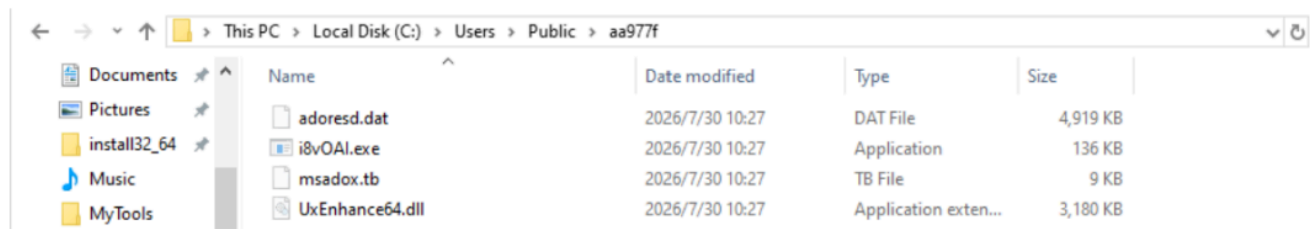


图 2 “白+黑”样本

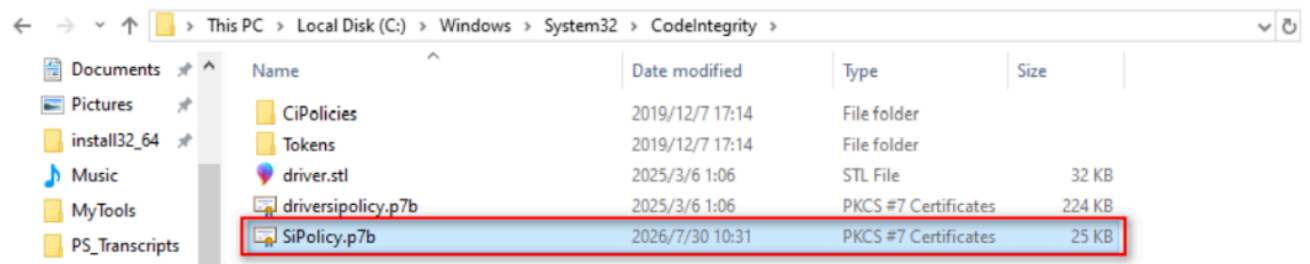


图 3 WDAC 策略文件

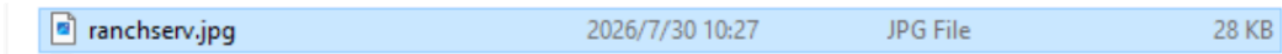


图 4 漏洞驱动文件

C:\Users\Public\{random char}下“白+黑”文件启动后会进行UAC Bypass提权以获得高权限，其主要功能是写入WDAC策略，以服务的形式加载漏洞驱动，并从阿里云OSS拉取下一阶段恶意文件，写入 C:\Program Files (x86) 下。

HKLM\System\CurrentControlSet\Services					Thu Jul 30 10:31:23 2026
☒ AWEAlloc	AWE Memory Allocation Driver: Driver for...	(Verified) Lagerkvist Tekniksk Radgi...	C:\Windows\system32\DRIVERS\awealloc.sys		Wed Feb 5 18:54:38 2020
☒ BthA2dp	Microsoft Bluetooth A2dp driver: Bluetoo...	(Not Verified) Microsoft Corporati...	C:\Windows\System32\drivers\bthA2dp.sys		Sat Dec 7 17:07:47 2019
☒ BthHfEnum	Microsoft Bluetooth Hands-Free Profile d...	(Not Verified) Microsoft Corporati...	C:\Windows\System32\drivers\bthhenum.sys		Sat Dec 7 17:07:47 2019
☒ iaLPSS_GPIO	Intel(R) Serial IO GPIO Controller Driver: I...	(Verified) Intel Corporation - Clie...	C:\Windows\System32\drivers\iaLPSS_GPIO.sys		Sat Dec 7 17:07:50 2019
☒ ImDisk	ImDisk Virtual Disk Driver: Disk emulation...	(Verified) Lagerkvist Tekniksk Radgi...	C:\Windows\system32\DRIVERS\imdisk.sys		Wed Feb 5 18:54:38 2020
☒ npcap	Npcap Packet Driver (NPCAP): Npcap Pa...	(Verified) Nmap Software LLC	C:\Windows\system32\DRIVERS\npcap.sys		Thu Aug 29 06:42:38 2024
☒ ProxifierDrv	ProxifierDrv: ProxifierDrv Callout Driver	(Verified) VENTIOBYTE SL	C:\Windows\System32\drivers\ProxifierDrv.sys		Mon Sep 25 13:20:56 2023
☒ SysmonDrv	SysmonDrv: System Monitor driver	File not found: SysmonDrv.sys			
☒ TCLService	TCLService:	(Verified) Adlice	C:\Windows\Temp\ranchserv.jpg		Thu Jul 30 10:27:13 2026

图 5 漏洞驱动加载

This PC > Local Disk (C:) > Program Files (x86) > IgGQrZ					
	Name	Date modified	Type	Size	
	IgGQrZ.exe	2026/7/30 10:31	Application	146 KB	
	image.png	2026/7/30 10:31	PNG File	4,995 KB	
	thumbs.db	2026/7/30 10:31	Data Base File	359 KB	
	XPSLOG.dll	2026/7/30 10:31	Application exten...	4,701 KB	

图 6 从 OSS 拉取的文件

其中ranchserv.jpg是非常经典的TrueSight V2.0.2 内核驱动，成功加载后可向攻击者提供内核层面的进程终止、文件读写、注册表清除及APC注入等能力，进而实现杀软及EDR等安全工具的致盲。

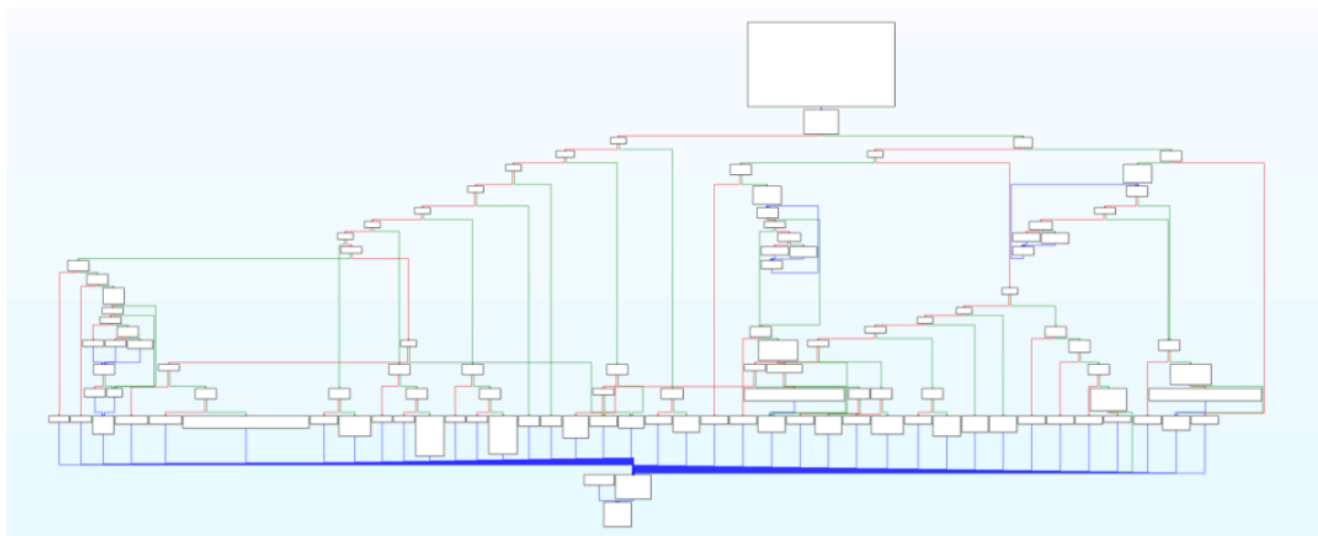


图 7 驱动能力主分发器

从OSS下载的文件（IgGQrZ.exe）依旧采用“白+黑”的手法，其主要功能是解密payload（Gh0stRAT）并注入内存回连攻击者C2，同时从阿里云 OSS 下载下一阶段恶意程序，写入

C:\ProgramData\{random char}，并通过注册表建立持久化。在致盲层面其通cmd.exe 执行系统致盲命令（禁用 Defender/Windows Update、删除卷影副本、修改host文件）。

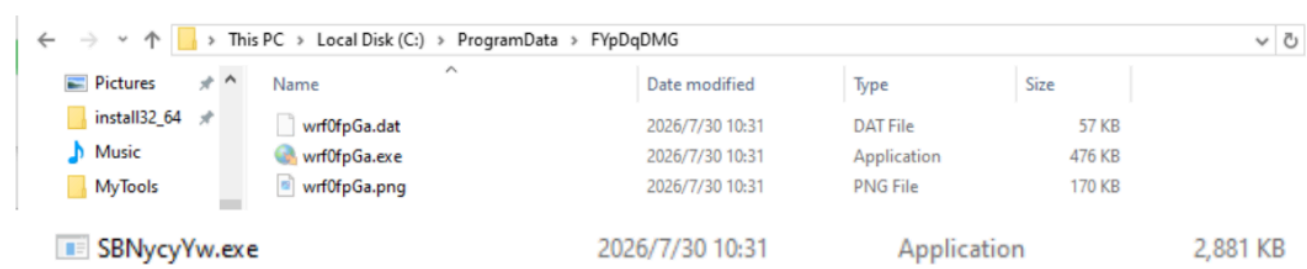


图 8 从 OSS 拉取的下一阶段木马

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				
☒ Alibaba SecurityHealtha	Philips Speech Driver Client Configuration	(Verified) Speech Processing Solut...	C:\Program Files (x86)\lgGQz\lgGQzZ.exe	Thu Jul 30 10:31:40 2026
☒ BinDiffPerUserSetup	Everything	(Verified) Google LLC	C:\Program Files\BinDiff\bin\bindiff_config_setup.exe	Thu Jul 30 10:31:25 2026
☒ Everything	Everything	(Verified) voidtools	C:\Program Files\Everything\Everything.exe	Mon Sep 25 05:20:08 2023
☒ Tencent SecurityHealth		(Not Verified)	C:\Users\Public\as977f\Br\OAL.exe	Thu Aug 1 17:13:54 2024
☒ VMware User Process	VMware Tools Core Service	(Verified) VMware, Inc.	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	Tue Oct 3 03:00:36 2023

图 9 持久化

```
$ hosts
C: > Windows > System32 > drivers > etc > $ hosts
1 # Copyright (c) 1993-2009 Microsoft Corp.
2 #
3 # This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
4 #
5 # This file contains the mappings of IP addresses to host names. Each
6 # entry should be kept on an individual line. The IP address should
7 # be placed in the first column followed by the corresponding host name.
8 # The IP address and the host name should be separated by at least one
9 # space.
10 #
11 # Additionally, comments (such as these) may be inserted on individual
12 # lines or following the machine name denoted by a '#' symbol.
13 #
14 # For example:
15 #
16 #      102.54.94.97      rhino.acme.com      # source server
17 #      38.25.63.10      x.acme.com          # x client host
18
19 # localhost name resolution is handled within DNS itself.
20 #      127.0.0.1        localhost
21 #      ::1              localhost
22 127.0.0.1 weishi.360.cn
23 127.0.0.1 www.360.cn
24 127.0.0.1 sd.360.cn
25
```

图 10 修改 host 文件

wrf0fpGa.exe是一个基于TrueUpdate的挖矿安装程序，其会伪装成xshell安装程序，实际向远端OSS请求名为“page-404.png”的文件并将其落地于C:\ProgramData\{random char}，此外攻击者还会通过计划任务实现新落地文件的持久化。

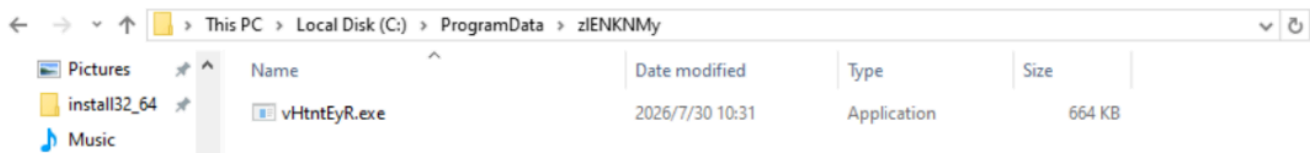


图 11 落地的挖矿木马

OneDrive Startup Task-5-1-5-21-2043037609-404845068-386637...			File not found: C:\Users\MyEnvi\AppData\Local\Microsoft\OneDrive\25.075.0420.0002\OneDriveLaunch...	
Seamless Delegation Workflow Prioritization	vision inventory with organize implement...	(Verified) NetSarang Computer, Inc.	C:\ProgramData\FipDgDMG\unfipGa.exe	Thu Jul 30 10:31:55 2026
Software Powerful Capacity Governance	track stakeholder milestone schedule allo...	(Not Verified)	C:\ProgramData\SBHnyc\Yw.exe	Thu Jul 30 10:31:54 2026
Elcomsoft\Elcomsoft Updater Autostart	Elcomsoft Universal Updater	(Verified) Elcomsoft s.r.o.	C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Updater\updater-launcher.exe	Mon Aug 15 20:40:54 2026
GoogleSystem\Google\Updater\Google\UpdaterTaskSystem149...	GoogleUpdater Task System 149.0.7814.0	(Verified) Google LLC	C:\Program Files (x86)\Google\Google\Updater\149.0.7814.0\updater.exe	Wed Apr 29 02:41:29 2026
GoogleSystem\Google\Updater\Google\UpdaterTaskSystem151...	GoogleUpdater Task System 151.0.7910.0	(Verified) Google LLC	C:\Program Files (x86)\Google\Google\Updater\151.0.7910.0\updater.exe	Wed Jun 24 15:57:44 2026
Microsoft\Office\Office 15 Subscription Heartbeat	Task used to ensure that the Microsoft Of...	(Verified) Microsoft Corporation	C:\Program Files (Common Files)\Microsoft Shared\Office15\OLicenseHeartbeat.exe	Mon Oct 1 20:36:04 2012
Microsoft\Office\OfficeTelemetryAgent\allBack	该任务会启动 Office 遥测代理。该程...	(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\Office15\msosia.exe	Mon Oct 1 18:59:44 2012
Microsoft\Office\OfficeTelemetryAgent\LogOn		(Verified) Microsoft Corporation	C:\Program Files\Microsoft Office\Office15\msosia.exe	Mon Oct 1 18:59:44 2012
Microsoft\Windows\Application Experience\MainBackup	Collects program telemetry information i...	(Verified) Microsoft Corporation	C:\Windows\system32\compattelrunner.exe	Thu Mar 6 01:06:12 2025
Microsoft\Windows\Application Experience\MainBackup	Collects program telemetry information i...	(Verified) Microsoft Corporation	C:\Windows\system32\compattelrunner.exe	Thu Mar 6 01:06:12 2025
Microsoft\Windows\Application Experience\MainBackup	Collects program telemetry information i...	(Verified) Microsoft Corporation	C:\Windows\system32\compattelrunner.exe	Thu Mar 6 01:06:12 2025
Microsoft\Windows\Application Experience\Microsoft Compa...	Collects program telemetry information i...	(Verified) Microsoft Corporation	C:\Windows\system32\compattelrunner.exe	Thu Mar 6 01:06:12 2025
Microsoft\Windows\Application Experience\ProgramData\Upd...	Collects program telemetry information i...	(Verified) Microsoft Corporation	C:\Windows\system32\compattelrunner.exe	Thu Mar 6 01:06:12 2025
Tracking Efficiently Feedback	of plan hierarchy standardization executi...	(Not Verified)	C:\ProgramData\zIENKNMy\vHtntEy.exe	Thu Jul 30 10:31:57 2026

图 12 计划任务

(三) 挖矿阶段

落地挖矿木马以变形 UPX 壳保护，脱壳重建后确认是基于 XMRig 框架的 RandomX 多币种挖矿程序，由命令行参数 1776 触发激活；其通信采用“固定密钥流 XOR 混淆（512 字节硬编码表循环）→ Base64 → TLS”三层封装连接矿池，以规避流量监测。

```

if ( *(_DWORD *) (a1 + 936) != 3 )
    return -1;
if ( !(unsigned int) sub_1400D7C58(*(_QWORD *) (a1 + 1280)) )
    return -1;
if ( (unsigned __int64) (a2 - 1) > 0x2FFF )
    return -1;
v4 = (_QWORD *) (a1 + 1168);
if ( *(_BYTE *) (*(_QWORD *) (a1 + 1168) + a2 - 1) != 10 )
    return -1;
v5 = a2 - 1;
for ( i = 0; i < v5; ++i )
    *(_BYTE *) (*v4 + i) ^= *((_BYTE *) MiningPoolXorKeyTable + (i & 0x1FF));
sub_140028B08(v30, *v4, *v4 + v5);

```

图 13 混淆逻辑

```

if ( v5 )
{
    if ( (unsigned int) sub_140119FA8(a2, "stratum+tcp://", 14) )
    {
        if ( !(unsigned int) sub_140119FA8(a2, "stratum+ssl://", 14) )
        {
            *(_DWORD *) (a1 + 4) = 1;
            *(_BYTE *) a1 = 1;
LABEL_10:
            v6 = (_BYTE *) (v5 + 3);
            goto LABEL_11;
        }
        if ( (unsigned int) sub_140119FA8(a2, "socks5://", 9) )
            return 0;
    }
}

```

图 14 通信协议

```

{
  "id": 1,
  "jsonrpc": "2.0",
  "method": "login",
  "params": {
    "login": "x",
    "pass": "x",
    "agent": "/ (Windows NT 10.0; Win64; x64) libuv/1.49.2 msvc/2022",
    "algo": [
      "rx/0"
    ]
  }
}

{
  "jsonrpc": "2.0",
  "id": 1,
  "error": null,
  "result": {
    "id": "762127daba63c0e5",
    "job": {
      "blob": "10109e87acd30630d75a10144126bcd8e1e5de98f8ebcd596ce05d0f191c8a4d15091b1318b7c000000786b3",
      "job_id": "zفز1cA0dvmXbt3/0ZpEqf0ReI4IU",
      "target": "21020000",
      "algo": "rx/0",
      "height": 3729040,
      "seed_hash": "0e3b4521acd1982c62a99b6b76ad8504eaa80e164d8e9df3f047b1cf....."
    }
  }
}

```

图 15 解密后的部分挖矿流量

3

部分样本 IOC和 HASH

(一) C2基础设施：

1. gqsqoq.net
2. jnkous.net
3. lisyrf.net
4. wfmwsj.net
5. vxqvll.net
6. ufozdvn.net

(二) 样本HASH：

1.2e90e3aaa76f9bd0a5b9bfc83f92bdb51a1c42b9121d3f204fbcfb2b724a0f88

2.418102029f37211691325f75980476277c2ca3d66363f6ad4bc022e660ffd72f

3.f22ca2ecd01573012ff6a187b484f68b13bef285a590ae3c5f93a2c6a83a2f3c

4.b655766fc801ed8a07db3447bf6a8ab1ae12507eab3ebd560e662b2a804e2989

5.7b7ee0af580497220c90a5db42c5202a70c0c16007515bb7fde9d3ad6e341f7b

6.a72083135eaae2b4af0b30db51b46a03d44869d60a41f55cb2cf5f33fa992503

7.fafefa1bf9ffa5342341b92ee398499149958000bb3508a14e3458841b3e8f5c

4

加入SEID社区

(一) 简介

SEID是国资国企专属的国家级威胁情报共享实战平台，由国资国企在线监管安全运营中心倾力打造，集情报研判、样本分析、漏洞排查三大核心体系于一体，实时共享国资国企专属网络威胁信息，为国资国企网络安全运营工作保驾护航！

(二) 优势

SEID平台通过SD-WAN实现安全数据交互，集成沙箱设备为国资央企提供可疑样本上传和分析服务、为国资国企威胁情报共享和联防联控提供统一平台。集于国资国企在线监管安全运营中心5年积累的海量安全大数据、安全运营垂域大模型，它拥有：

最权威的国资央企威胁情报数据库：全面收集、高效整合国资央企情报资源和能力，实时汇聚来源于国资央企一线的实战威胁情报，通过国资国企网络信息安全在线监管平台验证，确保威胁情报的高鲜活性和高准确性。

高可信运营平台：通过国资国企白名单准入机制构建高可信生态，严格限定参与主体为国资国企成员，并实施文件隔离保护策略，确保共享环境安全可控。

(三) 使用注册

2.登录平台。使用专属账号，登录SEID

3.提交信息。按照平台规范，提交网络威胁信息

4.核验计分。内容审核完成后，自动核算积分

