



,Chrome



PEEP?????Chromium????????????????,?????????Smart Bookmarks????????????????,?????????
?,????????????????????????????????,?????30?????HTTP????????????????????,????????????????????
Cookie?????????,????????????????????????????, ??????????????,?????????nm_host.exe,??
Chromium?Native Messaging?????????Shell??,?
?????????,????????????????????

PEEP?????????????RedExt?????????GlassWorm????????????PEEP????????????Native
Messaging??





PEEP????????????

????	????/??	?????	????
????	????????????????? ??RDP	????????????????? ?????????	?????????????????
????	??PowerShell?? Secure Preferences ????????	?????????????????	Smart Bookmarks ?????????
????	???????/api/exfil	?????????????????	Cookie ???????????????
????	content.js????	?????????SaaS ?????	?????????????????
????	nm_host.exe?Native Messaging	??Windows/Linux??	?????????????????

??????PEEP

[illegible]

```

?????PEEP???install_silent.ps1?????????CRX?????????patch_secure_prefs.ps1??Secure
Preferences????????????????????????????????????????????????????????????IT?
ExtensionInstallForcelist?????????????????ID????????????????????????????

```

????????????30????????????????????background
 ??????????????????????????????????GitHub?????????Cookie???URL?????C2?507?????????
 HTTP??

content.jsNative MessagingAPI KeyO

```

????????????????????C2????????????nm_host.exe?Native Messaging?Chrome
????????????????????exe????????????SSH
????????????????????

```



□□□□□

?????Windows??

1. ??Chrome?Edge????????ID ejkndncpkdcjcikfhiamcdehdoegilbj????Smart Bookmarks
????????????????
2. ???? %LOCALAPPDATA%PEEPcrx ????????????????
3. ?????? nm_host.exe????????Native Messaging???? com.peep.lab????HKCU Software??
Chrome/Edge Native Messaging Hosts?????
4. ?? %LOCALAPPDATA%GoogleChromeUser_Data ? %LOCALAPPDATA%MicrosoftEdgeUser_Data ?
Secure Preferences?Preferences????????????????????????????????
5. ???? HKCUSoftwareGoogleChromeExtensions ?Edge????????????????ID???

?????Linux?? ??Chrome????????patch_secure_prefs_linux.py????????Native Messaging
manifest?????com.peep.lab?

?????:????????????????????????????????????Cookie
????????????????????????????????????ID???PowerShell????????????????????
install_silent.ps1????????????????Native Messaging????????%LOCALAPPDATA%PEEPcrx
??????

?????????????:

```
import json
import os
```

```
import platform
from pathlib import Path

SUSPICIOUS_ID = "ejkndncpkdcjcikfhiamcdehdoegilbj"
SUSPICIOUS_NAME = "smart bookmarks"
PEEP_CRX = Path(os.environ.get("LOCALAPPDATA", "")) / "PEEPcrx"

def chrome_prefs_roots():
    base = Path(os.environ.get("LOCALAPPDATA", ""))
    if platform.system() == "Windows":
        yield base / "Google/Chrome/User Data"
        yield base / "Microsoft/Edge/User Data"
    else:
        yield Path.home() / ".config/google-chrome"
        yield Path.home() / ".config/microsoft-edge"

def iter_extensions(prefs_file: Path):
    try:
        data = json.loads(prefs_file.read_text(encoding="utf-8"))
    except (OSError, json.JSONDecodeError):
        return
    settings = data.get("extensions", {}).get("settings", {})
    for ext_id, meta in settings.items():
        name = (meta.get("manifest", {}) or {}).get("name", "")
        yield ext_id, name, str(prefs_file.parent)

def main():
    hits = []
    for root in chrome_prefs_roots():
        for profile in root.glob("*/Preferences"):
            for ext_id, name, loc in iter_extensions(profile):
                if ext_id == SUSPICIOUS_ID or SUSPICIOUS_NAME in name.lower():
                    hits.append((ext_id, name, loc))
    if PEEP_CRX.exists():
        print(f"[!] ??PEEP????: {PEEP_CRX}")
    if hits:
        print("[!] ?????:")
        for row in hits:
            print("    ", row)
    else:
        print("[OK] ??Preferences???Smart Bookmarks / ?????ID")

if __name__ == "__main__":
    main()
```

??????? check_peep_ext.py????? python_check_peep_ext.py



IOC

C2 IP : 206.237.30.232
?: xfjcc.fun
?: 5001

()