

Cyber Threat Exchange Liechtenstein

26. September 2023



Real World Threat Intelligence

Tobias Balschun

Tec Lead Cyber Defense Services, balschun@avantec.ch

Agenda

- 1 Einleitung
- 2 Identity Intelligence
- 3 3rd Party Risk
- 4 Vulnerability Intelligence
- 5 Q&A



Cyber Threat Exchange Liechtenstein

26. September 2023

Identity Intelligence



Fragestellung:

- Gibt es kompromittierte Accounts von Mitarbeitern oder Kunden?

Woher kommen die Daten:

- Hacker-Foren
- Darkweb-Foren
- Malware Stealer Logs
- etc.

→ Sample Reports verfügbar am Round-Table

Customer Data Sample

```
{
  "subject": "Username",
  "dumps": [
    {
      "name": "Stealer Malware Logs 2023-08-31",
      "description": "This credential data was derived from stealer malware logs.",
      "downloaded": "2023-09-18T16:44:43.666Z",
      "compromise": {
        "exfiltration_date": "2023-08-31T19:35:00.000Z",
        "os": "Windows 10 Enterprise 64 Bit",
        "os_username": "Benny",
        "malware_file": "C:\\FRST\\taskhostw.exe",
        "computer_name": "DESKTOP-6000BHN",
        "antivirus": [
          "Windows Defender"
        ]
      },
      "infrastructure": {
        "ip": "90.146.147.219",
        "location": {
          "country": "AT"
        }
      },
      "first_downloaded": "2023-09-18T16:44:43.663Z",
      "latest_downloaded": "2023-09-18T16:44:43.666Z",
      "exposed_secret": {
        "type": "clear",
        "hashes": [
          {
            "algorithm": "SHA1",
            "hash_prefix": "913c"
          },
          {
            "algorithm": "SHA256",
            "hash_prefix": "ddcf"
          },
          {
            "algorithm": "NTLM",
            "hash_prefix": "02d0"
          },
          {
            "algorithm": "MD5",
            "hash_prefix": "f4bc"
          }
        ]
      }
    }
  ]
}
```

Username

Infection details

Credential age

MD5, SHA1, SHA256 and NTLM Hashes

```
{
  "details": {
    "properties": [
      "Letter",
      "Number",
      "UpperCase",
      "LowerCase",
      "AtLeast12Characters"
    ],
    "clear_text_hint": "DN"
  },
  "effectively_clear": true,
  "compromise": {
    "exfiltration_date": "2023-08-31T19:35:00.000Z"
  },
  "authorization_service": {
    "url": "https://...",
    "domain": "example.com",
    "fqdn": "example.com",
    "technology": "https",
    "protocols": [
      "https"
    ]
  },
  "malware_family": {
    "name": "Dark Crystal RAT",
    "id": "ZEgKiV"
  }
}
```

Password Properties

Login URL

Malware Family

4

Cyber Threat Exchange Liechtenstein

26. September 2023

Customer Data Sample

```
"subject": "██████████",
"dumps": [
  {
    "name": "Stealer Malware Logs 2023-06-11",
    "description": "This credential data was derived from stealer malware logs. These logs are",
    "downloaded": "2023-06-12T12:26:50.996Z",
    "compromise": {
      "exfiltration_date": "2023-06-11T13:44:33.000Z",
      "os": "Windows 10 Home Single Language [x64]",
      "os_username": "jstapi",
      "malware_file": "C:\\Users\\██████████\\AppData\\Local\\Programs\\NvNode\\Speech\\dwm.exe",
      "timezone": "UTC-06:00",
      "computer_name": "██████████"
    },
    "infrastructure": {
      "ip": "189.217.218.174",
      "location": {
        "country": "MX"
      }
    }
  },
  {
    "first_downloaded": "2023-06-12T12:26:50.996Z",
    "latest_downloaded": "2023-06-12T12:26:50.996Z",
    "exposed_secret": {
      "type": "clear",
      "hashes": [
        {
          "algorithm": "SHA1",
          "hash_prefix": "3900"
        },
        {
          "algorithm": "SHA256",
          "hash_prefix": "857b"
        },
        {
          "algorithm": "NTLM",
          "hash_prefix": "438b"
        },
        {
          "algorithm": "MD5",
          "hash_prefix": "c285"
        }
      ]
    }
  }
]
```

Username

Infection details

Credential age

MD5, SHA1, SHA256 and NTLM Hashes

```
"details": {
  "properties": [
    {
      "Letter",
      "Number",
      "UpperCase",
      "LowerCase",
      "AtLeast10Characters"
    },
    {
      "clear_text_hint": "Je"
    },
    {
      "effectively_clear": true
    }
  ],
  "compromise": {
    "exfiltration_date": "2023-06-11T13:44:33.000Z"
  },
  "authorization_service": {
    "url": "██████████",
    "domain": "██████████",
    "fqdn": "██████████",
    "technology": [
      {
        "name": "Citrix NetScaler Access Gateway",
        "id": "Qtqec7",
        "category": "CAfzv"
      },
      {
        "name": "VPN",
        "id": "CAfzv"
      }
    ],
    "protocols": [
      "https"
    ]
  },
  "malware_family": {
    "name": "Vidar",
    "id": "YuDLEm"
  },
  "cookies": [
    {
      "dns": "██████████",
      "name": ".ga",
      "http": true,
      "expiration": "2024-06-07T17:32:58.000Z",
      "secure": true
    },
    {
      "dns": "██████████",
      "name": ".gid",
      "http": true,
      "expiration": "2023-05-05T17:32:58.000Z",
      "secure": true
    }
  ]
}
```

Password Properties

Login URL

Malware Family

Cookies

Web UI (Sample)

Exposures

Exposures Search Logout

Domains All Type All Technologies All Malware Family All Show All

Exposure Timeline

Top Domains

Domain	Employees Credentials
██████████	510
██████████	238
██████████	1

Credentials Stealer Malware

Malware	Total
██████████	7.77K
██████████	1

Technologies Exposed

Technology	Total
██████████	35
██████████	322
██████████	129
██████████	108

Exposures Detail

Field	Value
Name	Stealer Malware Logs 2022-08-19
Identity	██████████
Domain	██████████
Authorization URL	https://██████████.com/member.php
Description	This credential data was derived from stealer malware logs. These logs are legally obtained from multiple underground sources. Most data is available within 48 hours of exfiltration date for each specific exposure.
Detection Date	Apr 20, 2023, 07:08
Exfiltration Date	Jun 19, 2022, 16:00
Type	Clear
Hashes	Algorithm: SHA1 Hash: d6c70ca143c9c9e94b5ed7b2e7c3a9a165025 Algorithm: SHA256 Hash: fc7e090d771af6d69ef028bce0079c488b6fed688796 Algorithm: NTLM Hash: 5d08e1f6d20c4487d9c9da7e4dfb1 Algorithm: MD5 Hash: 98646341215a9dccc2c7519b7edaaf
Properties	Letter, Number, UpperCase, LowerCase, AtLeast10Characters
Password	Lu*****
Effectively Clear	True
Malware Family	██████████
Compromised Host	Operating System: Windows 10 Enterprise x64 OS User Name: Tessa File Path Location: UNKNOWN

Cyber Threat Exchange Liechtenstein

26. September 2023

3rd Party Risk



- Monitoring von Lieferanten u/o Partner-Unternehmen
 - Früh-Erkennung von Breaches oder anderen Security-Issues
 - Hat das einen Impact auf mein Unternehmen? Müssen Massnahmen eingeleitet werden?
 - VPN Tunnel oder andere Kommunikations-Wege schliessen?
 - Supply-Chain überprüfen?
- Auswahl-Kriterium für zukünftige Partner/Lieferanten?

→ Demo

Vulnerability Intelligence



- Fragestellung
 - Welche Schwachstellen soll ich priorisiert behandeln?
 - PoC Code
 - Threat Actors
 - Erfolgreiche Breaches
 - Gibt es Argumente für eine Down-Time?
 - Gibt es evtl. unbekannte Schwachstellen (noch keine CVE)
- Risiko basierter Ansatz
- Alerts gemäss definierten Watchlists



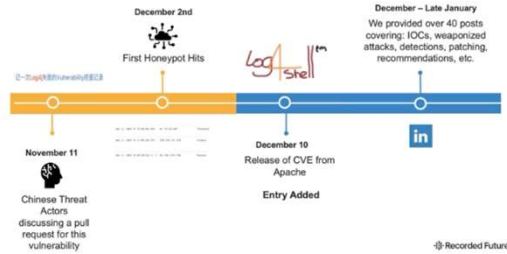
Cyber Threat Exchange Liechtenstein

26. September 2023

Vulnerability Intelligence



Log4Shell (CVE-2021-44228)



Cisco IOS XR Software (CVE-2022-20821)

