Tracing the Intrusion: Unveiling the Covert Trails of Infostealer Malware Ecosystems

Pavan Karthick M
Threat Researcher, CloudSEK
Agenda

- Introduction
- What damage can info stealers do
- Case study – Major Cyber attack
- Traffers & their Ecosystem
- Delivery Mechanisms & Evolution
- Trends
- Motivation
- Mitigation & Concluding Notes
5 Most Dangerous Cyber Attacks according to SANS

- SEO Boosted attacks
- Malvertising
- Developers as target
- Offensive uses of AI
- Weaponizing AI for Social Engineering

Ref: https://www.darkreading.com/attacks-breaches/sans-lists-top-5-most-dangerous-cyberattacks-in-2023
Introduction

- Infostealer – What is it?
- What enables it?
- Infostealer capabilities
  - Packers – Hides payload
  - Loaders – Drops payload
  - Defender, AMSI and EDR Bypasses
  - Exploiting CVEs - They are on track with latest security trends!
  - Updated with exfiltrating data of most used software.
What happens if you are infected

● Data gets compromised across synced devices.
● Exploited multiple times by multiple threat actors.
● Victim’s browser is mimicked and IP impersonation to bypass 2FA, IP based login
Case Study

- Cyber attack was on an organization with ~$30B Revenue
- Minimal Skill
- Maximum Damage
- Used by every TA

Social Engineering
  - VPN Credentials
  - Scanned Intranet
  - Internal Access
  - Network "Share"
    - PS Scripts
      - Hardcoded admin creds

Logs from Marketplaces were utilized to gain access

PAM leads to AWS, GSuite, Multiple internal sites
Traffer Ecosystem

Log Checker

Buyers

Market

Traffer Admin

Malware Developer

Crypter Developer

Traffer Resources

Telegram Bot with capabilities of:
1. Automated Builds
2. User Manual
3. SEO Panel,
4. Log Checker Software
5. Proxy kit
6. Youtube Uploader

Traffers
Cheap Domains (Behind Cloudflare)
Redirector 1
Redirector 2
Redirector 1x
Redirector 2x
Shortners
Malware Archive

SEO Enhanced
Amazing Templates
Crawling Detection
Anti-Analysis
Mimicking legit sites
Delivery 2 – Contd..

- Video Gets Posted
- Redirects to Download Service
- Archive with Massive compression ratio
- Infostealer Execution
- Data Exfiltration
- Data Sale
- Exploitation
- C2

YouTube

C:\Users\mpkar\Downloads\App-Zone_pass2023.rar

1. PROPAMAT: 130,316,387 bytes, 55,174,528 bytes, Modified: 2023-08-21
2. Templates: 592,916 bytes, 191,680 bytes, Modified: 2023-08-13
4. Installplus: 819,724,776 bytes, 7,731,392 bytes, Modified: 2023-08-21

1,872 views Premiered 7 hours ago #Filmora12 #filmora12Free #pastealaysdv
Delivery 3 - Mail Spam
Infection Chains keep Evolving with one Single goal ☓ To Steal Data

- Usage of AI Generated Voice overs and Personas to feature in their videos
- Constantly evolving & diverse tactics
- Achieving business continuity by usage of compromised accounts
  - To run their infrastructure of hosting malware
  - Deceive users into believing the content is genuine
Motivation?

- Lot of scope to earn for a skilled TA
- Zero to Hero training by TA for TA
- Less knowledge of the public around malicious software
- Money 😱
  - Potential > $100k USD
What Do We Do?

- Continuous Evolution & Automation in proliferation requires same proactive Automated Detection and Mitigations
- IoCs & YARA rules seem useless due to the sheer volume of infection chains possible in terms of Domains, samples, C2s.
  - Enforcing MFA & Strict session limits (For internal websites)
  - Organizations following BYOD policy should add windows policies locally which can prevent storage of passwords on browser.
  - Regular awareness training.
  - Paid software should be made available.
THANK YOU!