Digisuraksha Cybersecurity Internship 2025

Intern Name: Dhairya Kumar Patel
Intern ID: 445
Date: July 2025

Section 1: Malware Overview

Trojan.GenericKD.6114449 is a heuristic/generic detection used by antivirus tools to flag potential Trojan behavior. This type of malware typically masquerades as legitimate software and can execute a wide variety of malicious actions such as keylogging, creating backdoors, downloading additional payloads, or participating in botnet activity. It has been associated with phishing email campaigns and ZIP file droppers.

Section 2: File Metadata

- SHA-256: e7def648f10c23a32125e7d663327c87b092f2aeb71c87af19a6c4c03828e7d8
- File Type: Likely PE32 executable (Windows 32-bit)
- File Size: Unknown
- Compilation Timestamp: Not available (requires original binary)

Section 3: PE Structure Analysis

- Expected PE sections: .text, .data, .rdata, .rsrc
- No export functions typical for EXE
- High entropy values likely indicate packing or obfuscation
- Unusual section names or abnormal sizes might also suggest use of packers

Section 4: Static Strings Analysis

- Suspicious filenames like '25.tmp', or 'DHL_Report_*.zip'
- Potential DGA-based C2 domains like '*.ksmvryodp.com'
- Registry key references: 'Software\Microsoft\Windows\CurrentVersion\Run'

• Presence of HTTP/SMTP commands, proxy settings, and encoded URLs

Section 5: Import Table Analysis

• Kernel32.dll (file I/O, process/thread control)

• Advapi32.dll (registry manipulation)

• WinInet.dll or ws2_32.dll (network communications)

• Shell32.dll, User32.dll (GUI manipulation or social engineering)

• Crypt32.dll (possible encryption or obfuscation)

Section 6: Packing and Obfuscation Indicators

• High section entropy (~7.98) suggests packer usage

• Encrypted or encoded strings are commonly used

• Dynamic API resolution might bypass static IAT analysis

• Packers like UPX or Themida might be present

Section 7: YARA Rule (Example)

```
rule Trojan_GenericKD_6114449 {
   meta:
      description = "Detects Trojan.GenericKD.6114449 sample"
      author = "Dhairya Kumar Patel"
      hash = "e7def648f10c23a32125e7d663327c87b092f2aeb71c87af19a6c4c03828e7d8"
   strings:
      $s1 = "25.tmp" ascii
      $s2 = "ksmvryodp.com" ascii
      $s3 = { D1 FF 15 00 00 00 00 }
   condition:
      $s1 or $s2 or $s3
}
```

Section 8: Behavior Inferred from Static Indicators

• Persistence via registry Run key modification

• Proxy setting modifications to disrupt network access

• Email spamming functionality using SMTP commands

- Process injection into explorer.exe to remain stealthy
- Ransomware-like behavior in some variants (file encryption)

Section 9: Detection and Mitigation Strategies

- Deploy updated antivirus and EDR tools to match heuristic patterns
- Use YARA rules to detect known string or byte signatures
- Block known C2 domains and restrict external SMTP usage
- Train users against phishing and suspicious attachments
- Implement application allowlisting and limit user privileges
- Disconnect infected systems and run dedicated malware removal tools
- Restore from secure backups if ransomware behavior is confirmed