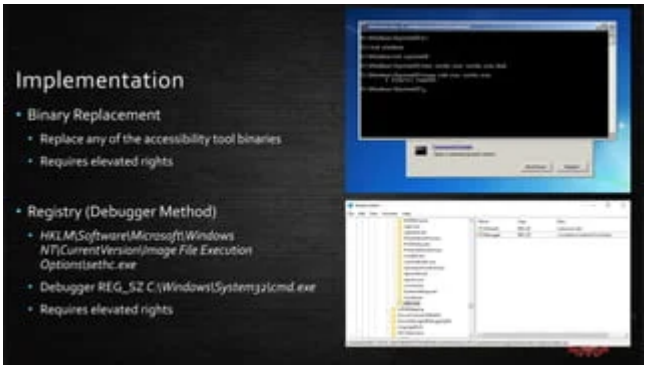
Sticky Keys to the Kingdom

Archived: 2026-04-06 01:03:33 UTC

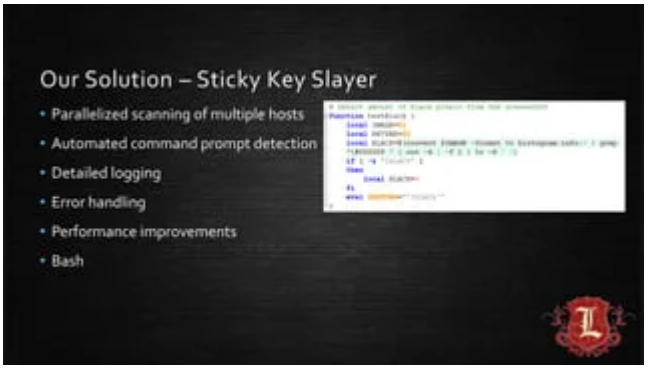



Windows Accessibility Tools
Binary
Description
How to access
Shift 5 times
Windows Key + U
Windows Key + Ctrl + O
Windows Key + Enter
Windows Key + P

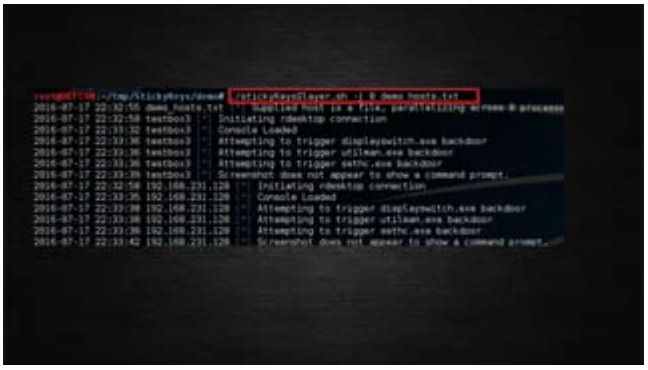

Limitations
Elevated access or offline system required
Replacing binary must be Digitally Signed
Replacing binary must exist in \System32\
Replacing binary must exist in Windows "Protected File" list
You can't use any old Binary, but you can cmd.exe /c file.bat

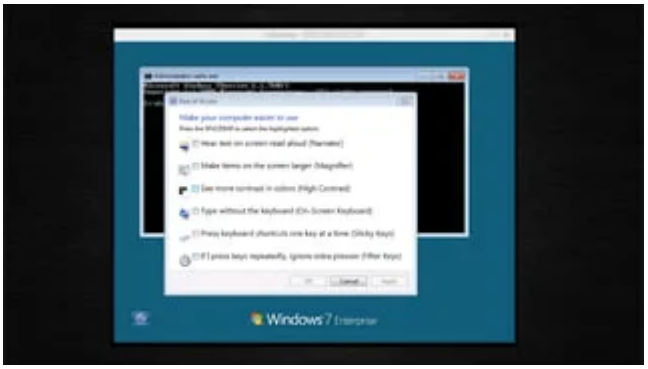

Background
While working with an Incident Response Team:
Uncovered dozens of vulnerable hosts via file checks
Identification was done from the filesystem side
Missed the debugger method
Missed any unmanaged boxes
Needed a network-based scanner


Background
We wanted to write out own network-based tool
Started down the JavaRDP/Python Path
Ran across @ztgrace's PoC script, Sticky Keys Hunter
It worked, and was a great starting point
Similar to "Peeping Tom"
Opens a Remote Desktop connection
Sends keyboard presses
Saves screenshot to a file
To do list including automatic command prompt detection and multi-threading


Our Solution – Sticky Key Slayer
• Parallelized scanning of multiple hosts
• Automated command prompt detection
• Detailed logging
• Error handling
• Performance improvements
• Bash

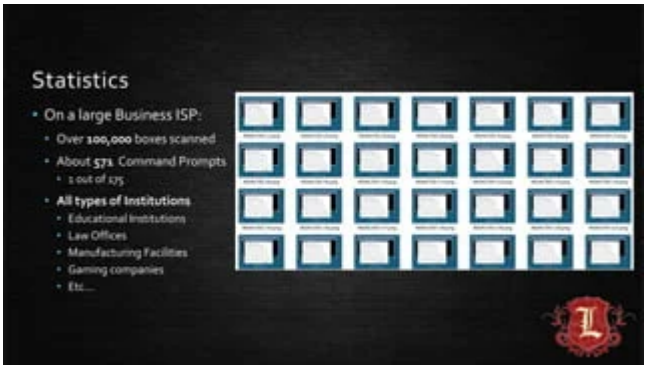

DEMO
VIDEO:
HTTPS://WWW.YOUTUBE.COM/WATCH?V=JY4HGGA1FYI

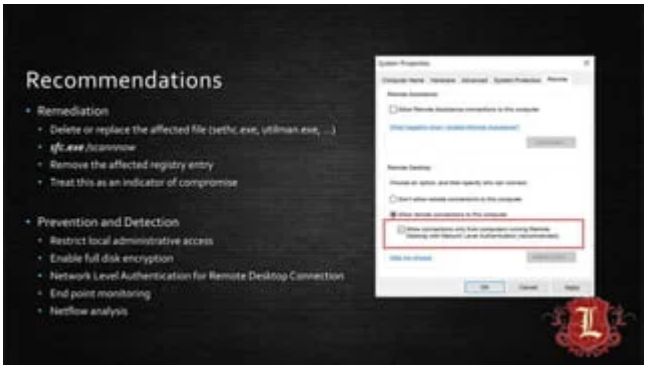


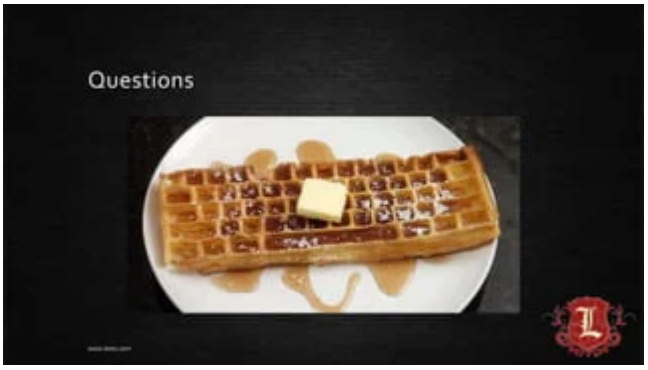

Windows 7 Enterprise


Tools Usage
./stickyKeysSlayer.sh -v -j 8 -t 10 targetlist.txt
-v
Verbose output
-j <num_of_jobs>
Jobs to run (defaults to 1)
-t <time_in_seconds>
Timeout in seconds (defaults to 30 seconds)
targetlist.txt
Hosts list delimited by line
1 192.168.0.2
2 192.168.77.23
3 172.16.9.44
4 172.16.9.45
5 172.16.9.46
6 172.16.9.47
7 172.16.9.48
8 172.16.9.49
9 172.16.9.50


Limitations
Ties up a Linux VM while scanning
Needed for window focus and screenshotting
Will not alert on anything that is not cmd.exe
Ran across taskmgr.exe, mmc.exe, other custom applications







More Related Content

PDF

Upping the APT hunting game: learn the best YARA practices from Kaspersky

PDF

A Year in the Empire

PDF

aclpwn - Active Directory ACL exploitation with BloodHound

PDF

SEH overwrite and its exploitability

PDF

Aem dispatcher – tips & tricks

PDF

Windows attacks - AT is the new black

PPTX

PSConfEU - Offensive Active Directory (With PowerShell!)

PPTX

Here Be Dragons: The Unexplored Land of Active Directory ACLs

What's hot

PDF

Secure Coding principles by example: Build Security In from the start - Carlo...

PPTX

Deep dive into Java security architecture

PPTX

Secure coding practices

PPT

iOS Application Pentesting

PDF

Monitoring your Python with Prometheus (Python Ireland April 2015)

PPTX

Netcat - A Swiss Army Tool

PDF

Automation with ansible

PDF

Windows Threat Hunting

PDF

CNIT 126: 10: Kernel Debugging with WinDbg

PDF

OpenStack keystone identity service

PPTX

Bridging the Gap

PDF

Thick Client Penetration Testing.pdf

PPTX

Building secure applications with keycloak

PPTX

Malware Static Analysis

ODP

Graylog

PPTX

RACE - Minimal Rights and ACE for Active Directory Dominance

PDF

Owasp zap

PPTX

Vault

PPTX

Intro to Pentesting Jenkins

PDF

Hunting for Privilege Escalation in Windows Environment

Viewers also liked

PPTX

Hacking Access Control Systems

PPTX

Getting Started in Information Security

PPTX

Metasploit for Web Workshop

PDF

Zpusob Vyuky Marketingove Komunikace Na Pef Czu V Praze

DOC

Same Origin Policy Weaknesses

PDF

Paměťové techniky

PDF

Techniky učení

PDF

ePUB 3 and Publishing e-books

PPTX

Evaluating and Selecting a Learning Management System

PPTX

Windows 7 Security

PPTX

Access Controls Attacks

PPTX

Kali net hunter

PPT

Building An Information Security Awareness Program

Similar to Sticky Keys to the Kingdom

PDF

DEFCON 23 - Gerard Laygui - forensic artifacts pass the hash att

PDF

CNIT 121: 12 Investigating Windows Systems (Part 3)

PDF

Windows Attacks AT is the new black

PPTX

Owning computers without shell access 2

PDF

[2010 CodeEngn Conference 04] window31 - Art of Keylogging 키보드보안과 관계없는 키로거들

PDF

CNIT 152 12. Investigating Windows Systems (Part 3)

PDF

Hunting Lateral Movement in Windows Infrastructure

PDF

Ntxissacsc5 red 1 & 2 basic hacking tools ncc group

PPTX

Kheirkhabarov24052017_phdays7

PPTX

Горизонтальные перемещения в инфраструктуре Windows

PPT

Computer Forensics & Windows Registry

PDF

The Dark Side of PowerShell by George Dobrea

PPT

Computer Forensics & Windows Registry

PPTX

Illegal_File_Transferring_Memory_Forensics.pptx

PDF

CNIT 152: 12 Investigating Windows Systems (Part 2 of 3)

PPTX

Windows Malware Techniques

PPT

Malware forensics

PDF

Ever Present Persistence - Established Footholds Seen in the Wild

PPTX

So you want to be a security expert

PPTX

Cyber security and ethical hacking 9

Recently uploaded

PDF

Webinar Serie 2026 - HCL Notes 2026 durchleuchtet

PDF

Claude token security issues and overall security architecture

PPTX

Automating Form Validation and Verification with Multi-Modal LLMs

PDF

Empowering BFSI with ThousandEyes Real-Time Digital Performance Intelligence

PDF

2025 Infrastructure Resilience Blueprint

PDF

Energy Aware Combinatorial Optimization.pdf

PPTX

Automating GitHub Changelog Reading with AI Agentic Workflows for Faster Updates

PDF

The Agentic AI Foundation: Architecting Autonomous Systems for 2026 and Beyond

PDF

How a Gated Community Operates on Ground?

PPTX

Automating YAML Reusable Workflow Updates with GitHub Agentic Workflows for S...

PDF

Advanced Quantization Techniques for Large Language Models in 2026

PPTX

Comprehensive Introduction to Blockchain Technology for Maritime Sector Appli...

PDF

Scaling Applications from Prototype to Millions of Users: Architecture and Be...

PDF

Động cơ hơi nước đôi bản vẽ chi tiết và bản vẽ lắp

PPTX

Comprehensive Guide to Access Control and Security Vulnerabilities

PPTX

Hyper-Aether: AI-Native Computing with Dynamic VM Fabric Architecture

PPTX

Tutorial on Artificial Intelligence.pptx

PPTX

Challenges and Opportunities for Research Centers in the AI Era: Innovation, ...

DOCX

Comprehensive Guide to Buying Apple ID Accounts for Business and Personal Use

PDF

The Automated Factory A Strategic Blueprint for Modern Production Workflows

Sticky Keys to the Kingdom

- 1.

  Sticky Keys tothe Kingdom PRE-AUTH SYSTEM RCE ON WINDOWS IS MORE COMMON THAN YOU THINK DENNIS MALDONADO & TIM MCGUFFIN LARES

- 2.

  About Us • DennisMaldonado • Adversarial Engineer – LARES Consulting • Founder • Houston Locksport • Houston Area Hackers Anonymous (HAHA) • Tim McGuffin • RedTeam Manager – LARES Consulting • 10-year DEFCON Goon • DEFCON CTF Participant • Former CCDCTeam Coach www.lares.com

- 3.

  History • “How toResetWindows Passwords” websites • Replace sethc.exe or utilman.exe with cmd.exe • Reboot, Press Shift 5x orWIN+U • net user (username) (password) • Login! • Nobody ever cleans up after themselves • Can be used as a backdoor/persistence method • NoWindows Event Logs are generated when backdoor is executed

- 4.

  Implementation • Binary Replacement •Replace any of the accessibility tool binaries • Requires elevated rights • Registry (Debugger Method) • HKLMSoftwareMicrosoftWindows NTCurrentVersionImage File Execution Optionssethc.exe • Debugger REG_SZ C:WindowsSystem32cmd.exe • Requires elevated rights

- 5.

  Windows Accessibility Tools BinaryDescription How to access C:WindowsSystem32sethc.exe Accessibility shortcut keys Shift 5 times C:WindowsSystem32Utilman.exe Utility Manager Windows Key + U C:WindowsSystem32osk.exe On-Screen Keyboard Locate the option on the screen using the mouse C:WindowsSystem32Magnify.exe Magnifier Windows Key + [Equal Sign] C:WindowsSystem32Narrator.exe Narrator Windows Key + Enter C:WindowsSystem32DisplaySwitch.exe Display Switcher Windows Key + P C:WindowsSystem32AtBroker.exe Manages switching of apps

between desktops Have osk.exe, Magnify.exe, or Narrator.exe open then lock the computer. AtBroker.exe will be executed upon locking and unlocking

- 6.

  Limitations • Elevated accessor offline system required • Replacing binary must be Digitally Signed • Replacing binary must exist in System32 • Replacing binary must exist inWindows “Protected File” list • You can’t use any old Binary, but you can cmd.exe /c file.bat

- 7.

  Background • While workingwith an Incident ResponseTeam: • Uncovered dozens of vulnerable hosts via file checks • Identification was done from the filesystem side • Missed the debugger method • Missed any unmanaged boxes • Needed a network-based scanner

- 8.

  Background • We wantedto write out own network-based tool • Started down the JavaRDP/Python Path • Ran across @ztgrace’s PoC script, Sticky Keys Hunter • It worked, and was a great starting point • Similar to “PeepingTom” • Opens a Remote Desktop connection • Sends keyboard presses • Saves screenshot to a file • To do list including automatic command prompt detection and multi-threading

- 9.

  Our Solution –Sticky Key Slayer • Parallelized scanning of multiple hosts • Automated command prompt detection • Detailed logging • Error handling • Performance improvements • Bash

- 10.
- 15.

  Tools Usage • ./stickyKeysSlayer.sh-v -j 8 -t 10 targetlist.txt • -v • Verbose output • -j <num_of_jobs> • Jobs to run (defaults to 1) • -t <time_in_seconds> • Timeout in seconds (defaults to 30 seconds) • targetlist.txt • Hosts list delimited by line

- 16.

  Limitations • Ties upa LinuxVM while scanning • Needed for window focus and screenshotting • Will not alert on anything that is not cmd.exe • Ran across taskmgr.exe, mmc.exe, other custom applications

- 17.

  Statistics • On alarge Business ISP: • Over 100,000 boxes scanned • About 571 Command Prompts • 1 out of 175 • All types of Institutions • Educational Institutions • Law Offices • Manufacturing Facilities • Gaming companies • Etc…

- 18.

Recommendations • Remediation • Deleteor replace the affected file (sethc.exe, utilman.exe, …) • sfc.exe /scannnow • Remove the affected registry entry • Treat this as an indicator of compromise • Prevention and Detection • Restrict local administrative access • Enable full disk encryption • Network LevelAuthentication for Remote Desktop Connection • End point monitoring • Netflow analysis

- 19.

  Tool Release • Codeis on Github • https://github.com/linuz/Sticky-Keys-Slayer • Contribute • Report Issues • Send us feedback • Slides • http://www.slideshare.net/DennisMaldonado5/sticky-keys- to-the-kingdom • DemoVideo • https://www.youtube.com/watch?v=Jy4hg4a1FYI www.lares.com

- 20.

Editor's Notes

- #2 Tim
- #3 Tim
- #4 Tim Find better top screenshot
- #5 Tim
- #6 Tim
- #7 Tim
- #8 Tim
- #9 Tim
- #10 Dennis
- #11 Dennis
- #13 Dennis
- #14 Dennis
- #15 Dennis
- #16 Dennis Write this slide on tool usage. Help stuff
- #17 Dennis
- #18 Tim
- #19 Dennis
- #20 Dennis Write this slide
- #21 Dennis
