Solution Brief

Safeguarding Against Pinkslipbot

W32/Pinkslipbot is a self-propagating malware family created to steal personal and financial data from its victims. This malware allows complete control of infected systems through a command-based backdoor operated by the control server as well as a virtual network computing–based backdoor. Pinkslipbot can also spread to other systems within the environment through network shares and can communicate to its control server to download updated versions of itself.

Pinkslipbot was initially identified in 2007, but the group that created it has maintained the code base by adding incremental updates before releasing a new version into the wild every few months.

Data stolen by Pinkslipbot enables an attacker to determine the location, organization, and owner of the infected system. The attacker could potentially sell this information (especially if it comes from a notable organization) to a third party and deploy targeted malware onto the compromised system after payment is made.

For an in-depth technical look into Pinkslipbot, please refer to the *McAfee Labs Threat Report: June 2016*. The report discusses the initial infection process, mechanisms of propagation, technical details, and general methods of protection.

Policies and procedures to protect against Pinkslipbot

Here are some general policies and procedures that can help you protect against Pinkslipbot.

To secure the perimeter, you should block unused ports on all egress points of the network, connection requests to and from known associated malicious IP addresses, and the use of network shares to stop Pinkslipbot's lateral movement. In most environments, you should also disable the Microsoft Windows AutoRun feature. It is vital to update Windows operating systems and applications to the latest patch levels, as well as update antimalware software to the latest version.

Unpatched systems allow vulnerabilities to be exploited. Successful patch management is necessary for every environment. When patches are issued by a vendor, they should be immediately tested, verified, and implemented. Where patching is not possible due to dependencies on an older version, there should be another mechanism in place to mitigate the exploitation of known vulnerabilities. Aggressive patch management is one of the most effective methods for mitigating the effects of Pinkslipbot and other malware.

intel Security

Although Pinkslipbot is delivered primarily via drive-by downloads from websites compromised by exploit kits, victims are usually directed to these sites from phishing emails. By tagging emails as "internal" or "external," users are more likely to identify spoofed or phishing emails and reconsider clicking unknown malicious links.

Pinkslipbot runs partially in memory, so it is not enough to simply patch systems, conduct a full scan, and run a malware-removal tool. Infected systems require a reboot to remove the malware from memory and a rescan to ensure that the system is clean. We also recommend using strong passwords to halt breaches by dictionary attacks, disabling AutoRun, and practicing the principle of "least privilege."

Pinkslipbot is an aggressive evolution of the infamous Zeus Trojan. A weak login password for a Windows system is enough to get infected by Pinkslipbot, even without exposure to an exploit kit or user interaction. Once a system is infected, any activity performed on the system is logged and sent to the attackers. With the introduction of custom, secure communication with its control servers, Pinkslipbot is becoming harder to detect and analyze. Its history suggests that it will become more dangerous with every succeeding iteration. By understanding your environment and implementing the policies and procedures we recommend, you can minimize the damage that Pinkslipbot can cause.

How Intel Security technology can help protect against Pinkslipbot

McAfee VirusScan Enterprise (VSE) and McAfee Endpoint Security (ENS) 10

McAfee VirusScan Enterprise and McAfee Endpoint Security 10 provide advanced antimalware protection for endpoint systems. McAfee VirusScan Enterprise has been superseded by McAfee Endpoint Security 10, which provides faster performance on an optimized platform. Intel Security DATs for McAfee VirusScan Enterprise and McAfee Endpoint Security 10 contain detection and cleaning capabilities for Pinkslipbot components. McAfee VirusScan Enterprise and McAfee Endpoint Security 10 provide multiple levels of protection through memory detection, antirootkit, behavioral, and static mechanisms. For additional layers of protection against new variants, you can implement Access Protection Rules to prevent Pinkslipbot from infecting systems.

- Create and test an Access Protection Rule to prevent any process from executing and creating any executable files in C:\Users*\AppData\Roaming\Microsoft**.exe.
- Create and test an Access Protection Rule to prevent cscrpit.exe and wscript.exe processes from reading, executing, and creating WPL files from the %LOCALAPPDATA%\Microsoft\ folder. These are usually JavaScript files. Blocking these files can prevent malware from downloading new versions.
- Create and test an Access Protection Rule to prevent cscrpit.exe and wscript.exe processes from reading and executing files from the %UserProfile% folder, where feasible.
- Create and test an Access Protection Rule for "updates_*new.cb", "upd_*.cb," and "updates*_new.cb" from executing and creating new files. These are usually used by Pinkslipbot configuration files. Blocking these files can prevent the malware from updating.
- Create and test an Access Protection Rule for ports 65200 to 65400 for the processes iexplorer.exe and explorer.exe. As Pinkslipbot injects itself into those processes, blocking those ports from being used by those processes prevents Pinkslipbot from communicating with its control server.
- Implement and test Access Protection Rules to prevent remote execution of autorun.inf files.

McAfee Host Intrusion Prevention (HIPS)
McAfee Host Intrusion Prevention protects systems from zero-day threats by combining a signature and behavioral intrusion prevention system with a dynamic, stateful firewall. Scheduled content updates protect systems from application and operating system vulnerabilities even before patches are available. Strengthen the security of an environment by enabling signatures to protect systems prevent many of the common methods that a piece of malware uses to exploit common software.

- Test and enable built-in McAfee Host Intrusion Prevention Signature 6010 Generic Application Hooking Protection.
- Test and enable built-in McAfee Host Intrusion Prevention Signature 6011 Generic Application Invocation Protection.
- Isolate systems infected by Pinkslipbot by assigning them a policy in which the firewall rule blocks all ports other than administration ports.

McAfee Endpoint Security 10 and McAfee Host Intrusion Prevention are included with McAfee Complete Endpoint Protection.

McAfee Web Gateway (MWG)
Drive-by downloads and links from emails are common ways that Pinkslipbot spreads. McAfee Web Gateway delivers high-performance web security, protecting systems from malicious websites. It can be deployed as either a dedicated hardware appliance or as a virtual machine image.

- Configure McAfee Web Gateway for spam filtering.
  - Spam filtering can protect against:
    - Malicious IPs
    - Malicious URLs
    - Email spam
- Enable GAM inspection.
- Enable McAfee GTI for URL and file reputation.
- Integrate with McAfee Advanced Threat Defense for sandboxing and zero-day detection.

McAfee Active Response (MAR)
McAfee Active Response provides continuous detection and response for systems targeted by advanced threats such as Pinkslipbot. Automated event monitoring allows you to find indicators of compromise that indicate a system is infected by malware.

- The presence of the following domains in a DNS cache may indicate a Pinkslipbot infection:
  - gpfbvtuz.org
  - hsdmoyrkeqpcyrtw.biz
  - lgzmtkvnijeaj.biz
  - mfrlilcumtwieyzbfdmpdd.biz
  - hogfpicpoxnp.org
  - qrogmwmahgcwil.com
  - enwgzzthfwhdm.org
  - vksslxpxaoql.com
  - dxmhcvxcmdewthfbnaspnu.org
  - mwtfngzkadeviqtlfrrio.org

  - jynsrklhmaqirhjrtygjx.biz
  - uuwgdehizcuuucast.com
  - gyvwkxfxqdargdooqql.net
  - xwcjchzq.com
  - tqxllcfn.com
  - feqsrxswnumbkh.com
  - nykhliicqv.org
  - ivalhlotxdyvzyxrb.net
  - bbxrsgsuwksogpktqydlkh.net
  - rudjqypvucwwpfejdxqsv.org
- Perform the following DNS cache query to determine whether systems have communicated with any of the known Pinkslipbot domains listed above.
  - DNSCache where DNSCache hostname equals "[Pinkslipbot Domain]"
- This query will return a list of established communications with Pinkslipbot domains from systems within the environment. You can easily identify which systems are communicating with those domains by clicking on the entry and showing the related systems.
- Use a local firewall such as McAfee ENS 10 or McAfee HIPS to quarantine systems affected by Pinkslipbot. To quarantine a system, assign a locked-down firewall policy to the system within McAfee ePO.
- Run a full McAfee ENS 10 or McAfee VSE On-Demand Scan of the system by assigning it an On-Demand Scan Task to Run Immediately within McAfee ePO. Wake up the agent to initiate the scan.

For Further Reading

McAfee Labs Threat Advisory: W32/Pinkslipbot

This advisory provides a detailed technical analysis of Pinkslipbot.

Intel Security Malware Webinar Series: Pinkslipbot

This video provides an overview of Pinkslipbot, regional and industry sector breakdowns, characteristics and symptoms, as well as prevention recommendations.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com