Untangling the Patchwork Cyberespionage Group

By Daniel Lunghi, Jaromir Horejsi, Cedric Pernet (words)

Published: 2017-12-11 · Archived: 2026-04-06 03:22:40 UTC

Updated as of October 9, 2018, 7:24PM PDT to remove Socksbot and update the appendix and technical brief; hat tip to Michael Yip of Accenture Security for an earlier research on Socksbot.

Patchwork (also known as Dropping Elephant) is a cyberespionage group known for targeting diplomatic and government agencies that has since added businesses to their list of targets. Patchwork's moniker is from its notoriety for rehashing off-the-rack tools and malware for its own campaigns. The attack vectors they use may not be groundbreaking—what with other groups exploiting zero-days or adjusting their tacticspredictions—but the group's repertoire of infection vectors and payloads makes them a credible threat.

We trailed Patchwork's activities over the course of its campaigns in 2017. The diversity of their methods is notable—from the social engineering hooks, attack chains, and backdoors they deployed. They've also joined the Dynamic Data Exchangenews article (DDE) and Windows Script Component (SCT) abuse bandwagons and started exploiting recently reported vulnerabilities. These imply they're at least keeping an eye on other threats and security flaws that they can repurpose for their own ends. Also of note are its attempts to be more cautious and efficient in their operations.

Who are Patchwork's targets?Patchwork targeted multiple sectors in China and South Asia. We also saw spear-phishing emails sent to organizations in the U.K., Turkey, and Israel.

The targets weren't just high-profile personalities, but also business-to-consumer (B2C) online retailers, telecommunications and media companies, aerospace researchers, as well as financial institutions (i.e., banks). They also targeted the United Nations Development Programme.

The group's motivations for targeting enterprises weren't clear; we don't construe them to be cybercriminal in nature, but espionage-related. Based on the malware used, they are more after mission-critical or confidential data than information they can monetize.

What did they use to infect their targets' systems?

Spear-phishing emails are their staple doorways into their targets, using emails that contained website redirects, direct links, or malicious attachments. For instance, Patchwork spoofed a news site to divert the visitors to socially engineered, malware-ridden documents. Spear-phishing emails with direct links to weaponized documents were hosted on Patchwork-owned servers whose domains are similar to legitimate sites. They misused email and newsletter distribution services to send these spammed messages.

Patchwork employed drive-by download tactics by setting up a fake Youku Tudou website, a social video platform popular in China. The would-be victim will be urged to download and execute a fake Adobe Flash Player update, which is actually a variant of the xRAT Trojan.

The group also phished for credentials to hijack their targets' emails and other online accounts. One of their phishing kits, for instance, copied a webpage from a legitimate web development company. The phishing pages can only be visited via the links in emails sent to would-be victims; otherwise, the user is redirected to the benign, mimicked webpage.

What kind of documents did Patchwork weaponize?Many of the documents we analyzed were from a directory Patchwork accidentally left open. The group used sociopolitical themes as social engineering hooks. The documents were laden with exploits for certain vulnerabilities:

- Rich Text Format (RTF) files that trigger an exploit for CVE-2012-1856, patched via MS12-060 last August 2012. CVE-2012-1856 is a remote code execution (RCE) vulnerability in the Windows common control MSCOMCTL, an ActiveX Control module
- PowerPoint Open XML Slide Show (PPSX) files exploiting Sandworm (CVE-2014-4114), an RCE vulnerability in Windows' Object Linking and Embedding (OLE) feature patched last October 2014
- PowerPoint (PPT) file exploiting CVE-2017-0199, an RCE vulnerability in Microsoft Office's Windows OLE, patched last April 2017
- PPSX files that exploit CVE-2017-8570, an RCE vulnerability in Microsoft Office patched last July 2017, which downloads a malicious Windows Script Component (SCT) file from a Patchwork-owned server then delivers the xRAT malware
- RTF files exploiting CVE-2015-1641, a memory corruption vulnerability in Microsoft Office patched last April 2015. After execution, it drops a dynamic-link library (DLL) that contains the Badnews backdoor, which is loaded and executed using DLL side-loading technique

Apart from exploit-laden documents, Patchwork also misused DDE to retrieve and execute xRAT in the infected machine. They also sent a document embedded with an executable, which downloads a decoy document and a backdoor, then executes the latter.

What were their payloads?
Patchwork deployed a miscellany of backdoors and information stealers, some of which they used exclusively:

- xRAT—a remote access tool whose source code is available on Github, which means anyone can clone and compile the project
- NDiskMonitor—a custom backdoor we believe to be Patchwork's own; it can list the infected machine's files and logical drives, as well as download and execute a file from a specified URL
- Badnews—a backdoor with potent information-stealing and file-executing capabilities; it can also monitor USB devices and copy targeted files to the C&C server
- File Stealers—Taskhost Stealer and Wintel Stealer target Microsoft Word, Excel, and PowerPoint documents (.doc, .docx, .xls, .xlsx, .ppt, and .pptx), Portable Document Format (.pdf) and RTF files, as well as email messages (.eml, .msg.); Patchwork also uses versions of file stealers written in AutoIt

What were Patchwork's operations like?

We found 30 to 40 IP addresses as well as domain names used by the group in 2017. Each server has a different purpose. Some are only meant to be C&C servers that collect data sent by the file stealers, and no domain name

points to those IP addresses. In some cases, the same server is used for C&C communication while also acting as a website hosting content copied from legitimate websites and propagating malware or weaponized documents. Other servers are used only to host phishing websites.

They misuse publicly available PHP scripts to retrieve files from the server without disclosing their real paths. While this could be for tracking purposes, it's more likely this was to deter researchers from finding open directories. On multiple occasions, we observed them temporarily removing a file so it could not be retrieved. Sometimes they replaced it with a legitimate file to dupe researchers. In some of their servers' homepages, they display a fake 302 redirection page to trick researchers into thinking the files are gone.

What can organizations do?

Patchwork is in a vicious cycle, given the group's habit of rehashing tools and malware. The more those are used, the likelier that they'd be incorporated in the group's arsenal. The takeaway for enterprises? The gamut of tools and techniques at Patchwork's disposal highlights the significance of defense in depth: arraying proactive defense to thwart threats at each level—from the gateways, endpointsproducts, and networksproducts to serversproducts.

Enterprises should keep operating systems and applications updatednews article—or employ virtual patchingnews article for legacy systems—to prevent security gaps and deter attackers from exploiting them. Firewallnews article, sandboxnews article, as well as intrusion detection and prevention systemsproducts help detect red flags in the network. Enforce the principle of least privilege: blacklist and secure the use of toolsnews- cybercrime-and-digital-threats usually reserved for system administrators, such as PowerShellnews article. Network segmentationnews article and data categorizationnews article help thwart lateral movement and further data theft, while behavior monitoring and application control/whitelisting block anomalous routines executed by suspicious files. And more importantly, secure the email gatewaynews- cybercrime-and-digital-threats. Patchwork may only be reusing vulnerability exploits and malware, but they're tried-and-tested—it only takes a susceptible layer to affect the whole chain.

Our in-depth analyses of Patchwork's campaigns—infection vectors, the weaponized documents and malware they deploy, and infrastructure—are in this ***technical brief***. The indicators of compromise are in this appendix.

Trend Micro Solutions

Trend Microproducts™ Deep Discoveryproducts™ provides detection, in-depth analysis, and proactive response to today's stealthy malware, and targeted attacks in real time. It provides a comprehensive defense tailored to protect organizations against targeted attacks and advanced threats through specialized engines, custom sandboxingnews article, and seamless correlation across the entire attack lifecycle, allowing it to detect threats delivered by Patchwork even without any engine or pattern update. Trend Micro™ Deep Securityproducts™, Vulnerability Protectionproducts, and TippingPoint productsprovide virtual patching that protects endpoints from threats that abuses unpatched vulnerabilities.

Patchwork also uses email as an entry point, which makes securing the email gateway important. Trend Micro™ Hosted Email Securityproducts is a no-maintenance cloud solution that delivers continuously updated protection to stop spam, malware, spear phishing, ransomware, and advanced targeted attacks before they reach the network. Trend Micro™ Deep Discovery™ Email Inspectorproducts and InterScan™ Web

Securityproducts prevent malware from ever reaching end users. At the endpoint level, Trend Micro™ Smart Protection Suitesproducts deliver several capabilities that minimize the impact of Patchwork's attacks.

These solutions are powered by the Trend Micro XGen™ securityproducts, which provides a cross-generational blend of threat defense techniques against a full range of threats for data centersproducts, cloud environmentsproducts, networksproducts, and endpointsproducts. It features high-fidelity machine learning to secure the gatewayproducts and endpointproducts data and applications, and protects physical, virtual, and cloud workloads.
