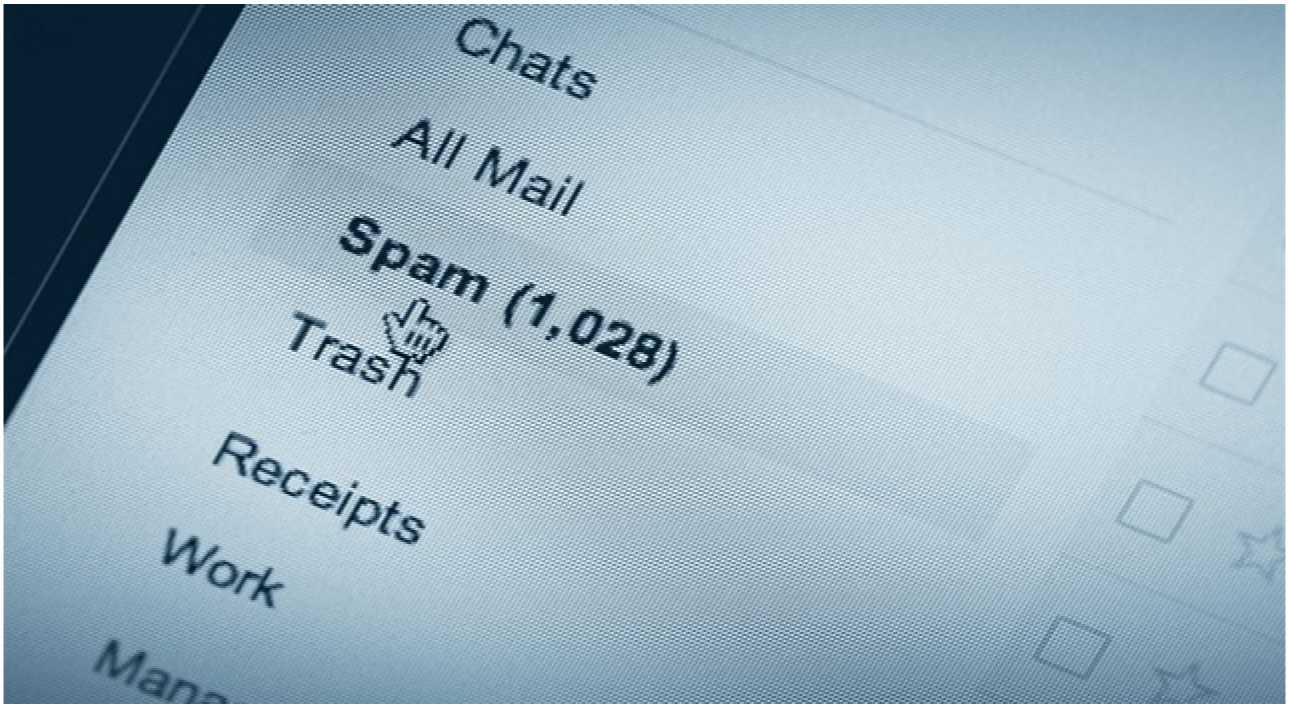
Spam Campaign Delivers Cross-platform RAT Adwind

blog.trendmicro.com/trendlabs-security-intelligence/spam-remote-access-trojan-adwind-jrat

July 11, 2017



Spam

Adwind/jRAT resurfaces in another spam campaign. This time, however, it’s mainly targeting enterprises in the aerospace industry, with Switzerland, Ukraine, Austria, and the US the most affected countries.

By: Rubio Wu, Marshall Chen, Ryan Maglaque July 11, 2017 Read time: (words)

Cybercriminals are opportunists. As other operating systems (OS) are more widely used, they, too, would diversify their targets, tools, and techniques in order to cash in on more victims. That’s the value proposition of malware that can adapt and cross over different platforms. And when combined with a business model that can commercially peddle this malware to other bad guys, the impact becomes more pervasive.

Case in point: Adwind/jRAT, which Trend Micro detects as JAVA_ADWIND. It’s a cross-platform remote access Trojan (RAT) that can be run on any machine installed with Java, including Windows, Mac OSX, Linux, and Android.

Unsurprisingly we saw it resurface in another spam campaign. This time, however, it's mainly targeting enterprises in the aerospace industry, with Switzerland, Ukraine, Austria, and the US the most affected countries.

Adwind operators are active

The spam campaign actually corresponds to our telemetry for JAVA_ADWIND. In fact, the malware has had a steady increase in detections since the start of the year. From a mere 5,286 in January 2017, it surged to 117,649 in June. It's notable, too, that JAVA_ADWIND detections from May to June, 2017 increased by 107%, indicating that cybercriminals are actively pushing and distributing the malware.

Adwind/jRAT can steal credentials, record and harvest keystrokes, take pictures or screenshots, film and retrieve videos, and exfiltrate data. Adwind iterations were used to target banks and Danish businesses, and even turned infected machines into botnets.

Notorious as a multiplatform do-it-yourself RAT, Adwind has many aliases: jRAT, Universal Remote Control Multi-Platform (UNRECOM), AlienSpy, Frutas, and JSocket. In 2014 we found an Android version of Adwind/jRAT modified to add a cryptocurrency-mining capability. The fact that it's sold as a service means this threat can be deployed by more cybercriminals who can customize their own builds and equip them with diverse functionalities.

Figure 1: JAVA_ADWIND detections from January to June, 2017 *Figure 2: Adwind's infection chain*

Spam campaign was deployed in two waves

The spam campaign we observed was deployed in two waves and is a classic example of social engineering. We saw the first on June 7, 2017 using a different URL to divert victims to their .NET-written malware equipped with spyware capabilities. The second wave was observed on June 14, and used different domains that hosted their malware and command and control (C&C) servers. Both waves apparently employed a similar social engineering tactic to lure victims into clicking the malicious URLs.

The spam email's message impersonates the chair of the Mediterranean Yacht Broker Association (MYBA) Charter Committee. The spam email's subject line, "Changes in 2017 – MYBA Charter Agreement", tries to cause a sense of urgency for potential victims. It uses a forged sender address, (*info[@]myba[.]net*) and a seemingly legitimate content to trick would-be victims into clicking the malicious URL.

Figure 3: Snapshot of the information sent to the C&C server *Figure 4: Snapshot of the spam email*

Analyzing Adwind's attack chain

The malicious URL will drop a Program Information file (PIF). PIFs contain information on how Windows can run MS-DOS applications, and can be launched normally like any executable (EXE). The file is written in .NET and serves as a downloader. The process spawned by the file kicks off the infection chain by first modifying the system certificate.

The URL we traced the malicious PIF file (TROJ_DLOADR.AUSUDT) to also contained various phishing and spam email-related HTML files. It’s possible that these are the landing pages from which victims are diverted to the malicious PIF file.

Figure 5: The downloader trying to modify the system certificate by calling Windows Application Programming Interface (API)

Figure 6: Snapshot showing a successfully modified certificate

After the certificate has been poisoned, a Java EXE, dynamic-link library (DLL) and 7-Zip installer will be fetched from a domain that we uncovered to be a file-sharing platform abused by the spam operators:

- hxxps://nup[.]pw/DJojQE[.]7z
- hxxp://nup[.]pw/e2BXtK[.]exe
- hxxps://nup[.]pw/9aHiCq[.]dll

The installer has a wrapper function, which are typically employed by RATs to call additional routines without sacrificing computational resources. The wrapper we analyzed was in a Java ARchive file format (JAR) that we have dubbed jRAT-wrapper (JAVA_ADWIND.JEJPCO), which will connect to a C&C server and drop the Adwind/jRAT in runtime.

Based on jRAT-wrapper’s import header, it appears to have the capability to check for the infected system’s internet access. It can also perform reflection, a dynamic code generation in Java. The latter is a particularly useful feature in Java that enables developers/programmers to dynamically inspect, call, and instantiate attributes and classes at runtime. In cybercriminal hands, it can be abused to evade static analysis from traditional antivirus (AV) solutions.

Figure 7: Code snapshot of the PIF file that downloads a wrapper (jRAT-wrapper), which then retrieves the payload

Figure 8: The domain nup[.]pw is a file-hosting server abused by the spam operators

Figure 9: Snapshot of an obfuscated Java class within jRAT-wrapper

Figure 10: jRAT-wrapper’s import header

Figure 11: The byte code we decompiled in jRAT-wrapper

jRAT-wrapper also tries to connect to another C&C IP address, 174[.]127[.]99[.]234:1033, which we construe to be from a legitimate hosting service that was abused by the attackers. jRAT-wrapper also uses Visual Basic scripts (VBS) to collect the system’s fingerprints, notably the installed antivirus (AV) product and firewall. It’s also coded to drop and execute the JAR file in the User Temp directory and copy malicious Java libraries to the Application Data folder. It will then drop a copy of itself in the current user directory and create an autorun registry for persistence.

However, we found that the IP address was already down during our analysis, preventing us from getting further information related to this IP address.

Figure 12: Malicious VBS file that gathers the infected system’s configurations

Figure 13: The properties of Adwind/jRAT

Security researcher Michael Helwig's rundown of jRAT-wrapper helped us decrypt the properties of the payload. The configuration file of the sample we analyzed indicated that the network traffic is designed to be hijacked to a proxy listen at the loopback address, 127[.]0[.]0[.]1:7777.

However, we were not able to record any proxy setting during our analysis as the C&C server that the jRAT-wrapper tried to connect to was already inaccessible. We can infer that the attackers intentionally shut down this C&C server. Once attackers successfully accomplish what they want in the infected system, they can shut it down to deter further analysis. It's also possible that the hosting service/ISP actually took it down for abuse.

In this instance, we can construe that a successful C&C communication entails the C&C server changing the proxy setting to the victims.

Figure 14: A part of Adwind's configuration file

Countermeasures

Adwind is a cross-platform, Java-based malware. This calls for a multilayered approach to security that covers the gateway, endpoints, networks, servers, and mobile devices. IT/system administrators and information security professionals, as well as developers/programmers that use Java should also adopt best practices for using and securing Java and regularly keep it patched and updated.

Adwind's main infection vector is spam email. This underscores the importance of securing the email gateway to mitigate threats that use email as an entry point to the system and network. Spam filters, policy management, and email security mechanisms that can block malicious URLs are just some of the solutions that can be used to help mitigate email-based threats. Users and IT/system administrators should also adopt best practices to help safeguard networks with bring-your-own device (BYOD) policies from threats like Adwind that can steal important data.

A crucial element in Adwind's attack chain is social engineering. This highlights the need to cultivate a cybersecurity-aware workforce and foster conscientiousness against email scams: think before you click, be more prudent when opening unknown or unsolicited emails, and be more aware of different social engineering tactics cybercriminals use. These best practices can significantly help reduce an organization's exposure to these malware.

Trend Micro Solutions

Trend Micro endpoint solutions such as Trend Micro™ Smart Protection Suites and Worry-Free™ Business Security can protect users and businesses from these threats by detecting malicious files, and spammed messages as well as blocking all related malicious

URLs. Trend Micro Deep Discovery™ has an email inspection layer that can protect enterprises by detecting malicious attachment and URLs.

Trend Micro™ Hosted Email Security 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. It protects Microsoft Exchange, Microsoft Office 365, Google Apps, and other hosted and on-premises email solutions.

Trend Micro™ OfficeScan™ with XGen™ endpoint security infuses high-fidelity machine learning with other detection technologies and global threat intelligence for comprehensive protection against advanced malware.

Indicators of Compromise

Files and URLs related to Adwind/jRAT:

- hxxp://ccb-ba[.]adv[.]br/wp-admin/network/ok/index[.]php
- hxxp://www[.]employersfinder[.]com/2017-MYBA-Charter[.]Agreement[.]pif
- hxxps://nup[.]pw/e2BXtK[.]exe
- hxxps://nup[.]pw/Qcaq5e[.]jar

Related Hashes:

- 3fc826ce8eb9e69b3c384b84351b7af63f558f774dc547fccc23d2f9788ebab4 (TROJ_DLOADR.AUSUDT)
- c16519f1de64c6768c698de89549804c1223addd88964c57ee036f65d57fd39b (JAVA_ADWIND.JEJPCO)
- 97d585b6aff62fb4e43e7e6a5f816dcd7a14be11a88b109a9ba9e8cd4c456eb9 (JAVA_ADWIND.AUJC)
- 705325922cffac1bca8b1854913176f8b2df83a70e0df0c8d683ec56c6632ddb (BKDR64_AGENT.TYUCT)

Related C&C servers:

- 174[.]127[.]99[.]234 Port 1033
- hxxp://vacanzaimmobiliare[.]it/testla/WebPanel/post[.]php

Tags

Spam | Endpoints | Research