CYBERATTACKS & DATA BREACHES

'Operation Shady RAT' Attackers Employed Steganography

Digital images hid commands controlling infected machines

Kelly Jackson Higgins, Editor-in-Chief, Dark Reading

August 11, 2011

4 Min Read

The attackers behind the "Operation Shady RAT" targeted cyberespionage hacks hid some of their activities behind digital images.

They used steganography, a relatively rarely deployed technique for hiding malicious code ata behind image files or other innocuous-looking files. In its analysis of Operation y RAT, Symantec found rigged images -- everything from images of a pastoral

waterside scene to a suggestive photo of a woman in a hat -- that were masking commands ordering the infected machines to phone home to the command-and-control (C&C) server.

The commands are invisible to the human eye because the bits in the image are actually made up of those commands. They're "mathematically built into the data representing the image," according to Symantec researchers in a recent blog post that includes examples of the images its researchers found.

Operation Shady RAT is a massive advanced persistent threat (APT)-type attack campaign that has been ongoing worldwide for five years and has stolen intellectual property from 70 government agencies, international corporations, nonprofits, and others in 14 countries. It was revealed last week by McAfee, which conducted an in-depth study of one of the C&C servers used in the attack.

Remaining under the radar is crucial for APT attackers. The Shady RAT attackers also deployed a tool called HTran that helps disguise their locations. Joe Stewart, director of malware research for Dell SecureWorks' counter threat unit research team, recently discovered a pattern in APT malware in which many of these attackers use HTran -- including the Operation Shady RAT attackers, he says.

Stewart actually was able to glean more information on the attackers' servers after discovering an error they had made in deploying the tool. That led him to the actual C&C servers used by the attackers, and he was able to narrow down the location of the main hubs to Beijing and Shanghai. "They are coming back and conversing with just a few networks in China," he says.

Meanwhile, Ben Greenbaum, senior principle software engineer at Symantec, says the use of steganography is not widespread in most attacks. "We have seen it in some pieces of prominent malware, but it's still in the minority," Greenbaum says.

It's unclear whether ATP attackers, overall, are increasingly employing this masking technology, but it definitely offers them another way to cover their tracks, security experts say.

"I believe use of steg by either an outsider in this case -- or an insider -- is part of the APT," says James Wingate, director of the steganography analysis and research center at Backbone Security. "It is a highly effective technique because the commands are sent covertly, and that would be exceptionally difficult to detect. Our tools would not detect this unless the Trojan was using a known steg app for which we had discovered a signature."

The targeted attacks started with legitimate-looking phishing emails that contained a link to a malicious file or URL. In one case, Defense contractors were targeted with a phishing email that had a link to a rigged spreadsheet, which contained a real list of high-level defense industry executives who attended a recent Intelligence Advanced Research Projects Activity (IARPA) event; this was also part of Operation Shady RAT.

That particular attack was studied by researchers at Invincea and ThreatGrid, who discovered a legitimate-looking domain that provided a ZIP archive to the attendee roster, complete with names of directors, presidents, and CEOs at major Defense and intelligence companies. But the XLS-looking file was actually an executable that extracted another custom program -- an HTTP client that beacons out to the C&C server, according to Anup Ghosh, founder and CEO of Invincea.

Symantec, meanwhile, says the images and HTML files used by the Shady RAT attackers appear legit, and their commands are actually encrypted. "In the versions of the Trojans that are downloading HTML files, the commands are hidden in HTML comments that look

like gibberish, but are actually encrypted commands that are further converted into base-64 encoding," according to Symantec.

Have a comment on this story? Please click "Add Your Comment" below. If you'd like to contact Dark Reading's *editors directly, send us a message.*

About the Author

Kelly Jackson Higgins, Editor-in-Chief, Dark Reading

Kelly Jackson Higgins is the Editor-in-Chief of Dark Reading. She is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise Magazine,...

You May Also Like

Cyberattacks & Data Breaches

Toyota Customer, Employee Data Leaked in Confirmed Data Breach

Iran Reportedly Grapples With Major Cyberattack on Banking Systems

Cyberattacks & Data Breaches

Aligning Breaches With MITRE ATT&CK Threat Model

More Insights

Webinars

DevSecOps/AWS
OCT 17, 2024

Social Engineering: New Tricks, New Threats, New Defenses
OCT 23, 2024

10 Emerging Vulnerabilities Every Enterprise Should Know
OCT 30, 2024

Simplify Data Security with Automation
OCT 31, 2024

More Webinars

Events

State of AI in Cybersecurity: Beyond the Hype

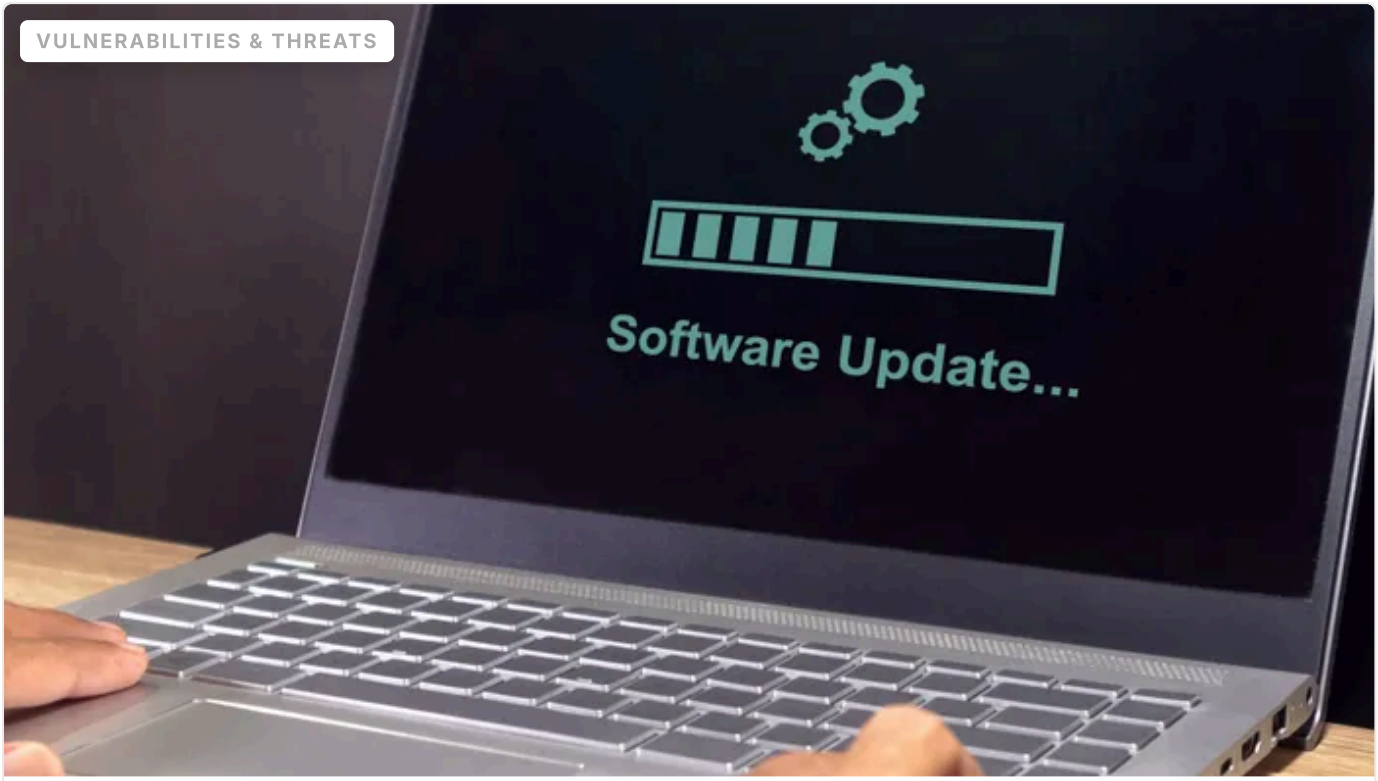
[Virtual Event] The Essential Guide to Cloud Management

Black Hat Europe - December 9-12 - Learn More

r - Canada's IT Security Conference Oct 22-24 - Learn More

More Events

Editor's Choice



5 Zero-Days in Microsoft's October Update to Patch Immediately

by **Jai Vijayan, Contributing Writer**

OCT 8, 2024 4 MIN READ

mba 2FA Cybercrime Kit Targets Microsoft 365 Users

by **Tara Seals, Managing Editor, News, Dark Reading**

OCT 9, 2024 1 MIN READ

Salt Typhoon APT Subverts Law Enforcement Wiretapping: Report

by **Tara Seals, Managing Editor, News, Dark Reading**

OCT 7, 2024 2 MIN READ

Reports

Managing Third-Party Risk Through Situational Awareness

JUL 31, 2024

2024 InformationWeek US IT Salary Report

MAY 29, 2024

More Reports

Webinars

DevSecOps/AWS
OCT 17, 2024

Social Engineering: New Tricks, New Threats, New Defenses
OCT 23, 2024

10 Emerging Vulnerabilities Every Enterprise Should Know
OCT 30, 2024

Simplify Data Security with Automation
OCT 31, 2024

More Webinars

White Papers

Insider Risk Programs: 3 Truths and a Lie

2024 Cloud Security Report

The State of Asset Security: Uncovering Alarming Gaps & Unexpected Exposures

A CISO's Guide to Geopolitics and CyberSecurity

SecOps Checklist

More Whitepapers

Events

State of AI in Cybersecurity: Beyond the Hype
OCT 30, 2024

tual Event] The Essential Guide to Cloud Management

OCT 17, 2024

Black Hat Europe - December 9-12 - Learn More

DEC 10, 2024

SecTor - Canada's IT Security Conference Oct 22-24 - Learn More

OCT 22, 2024

More Events

DARKREADING

Discover More With Informa Tech

Black Hat

Omdia

Working With Us

About Us

Advertise

Reprints

Join Us

NEWSLETTER SIGN-UP

Follow Us