The Initial Access Broker’s Toolbox – Remote Monitoring and Management

September 18, 2020

18 September 2020

Raveed Laeb, Product Manager and Victoria Kivilevich, Threat Intelligence Analyst

Updated on October 8, 2020 with a statement from Zoho Corporation

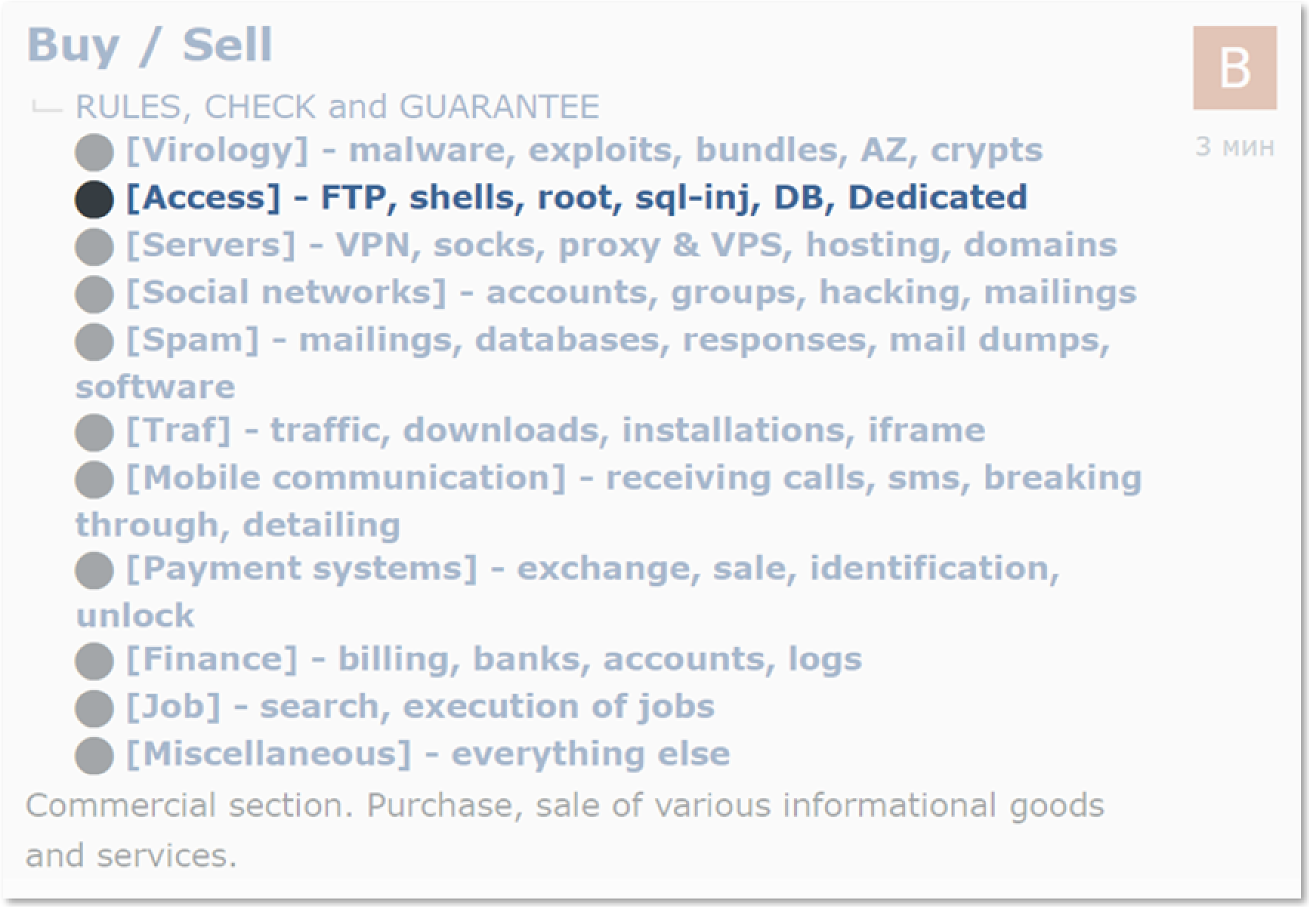
Bottom Line Up Front

- With the rise of Initial Access Brokers and threat actors selling remote access to compromised networks, Remote Monitoring and Management tools are becoming a lucrative target
- KELA noticed a cybercrime actor operating on a Russian-speaking forum, who lately offered dozens of accesses via an RMM tool KELA identified as Desktop Central – showcasing the threat organizations are facing
- Monitoring the types of network accesses offered for sale by Initial Access Brokers can hold significant intelligence value for defenders

50 Shades of Network Access

Remote monitoring and management (RMM) software is designed to help IT professionals manage networks – and as such, offer access and elevated permissions into multiple machines. As one can imagine, that kind of access may be very attractive to bad actors – and MSPs, the main driving force of RMM usage, have not escaped the targeting of ransomware actors. **Lately, KELA noticed RMM software being targeted as part of the compromise portfolio** of certain initial access brokers – either directly or via managed service providers.

A quick side trip, exploring the phrase “network access” as used by both KELA and threat actors, may be due. The term itself is very loosely defined; threat actors use it to describe multiple different vectors, permission levels and entry points. One can get an intuitive sense of this by looking at the sub-forum dedicated to trading network access on Exploit, a major Russian-speaking forum:



Buy / Sell

└─ RULES, CHECK and GUARANTEE

- ● [Virology] - malware, exploits, bundles, AZ, crypts
- ● [Access] - FTP, shells, root, sql-inj, DB, Dedicated
- ● [Servers] - VPN, socks, proxy & VPS, hosting, domains
- ● [Social networks] - accounts, groups, hacking, mailings
- ● [Spam] - mailings, databases, responses, mail dumps, software
- ● [Traf] - traffic, downloads, installations, iframe
- ● [Mobile communication] - receiving calls, sms, breaking through, detailing
- ● [Payment systems] - exchange, sale, identification, unlock
- ● [Finance] - billing, banks, accounts, logs
- ● [Job] - search, execution of jobs
- ● [Miscellaneous] - everything else

Commercial section. Purchase, sale of various informational goods and services.

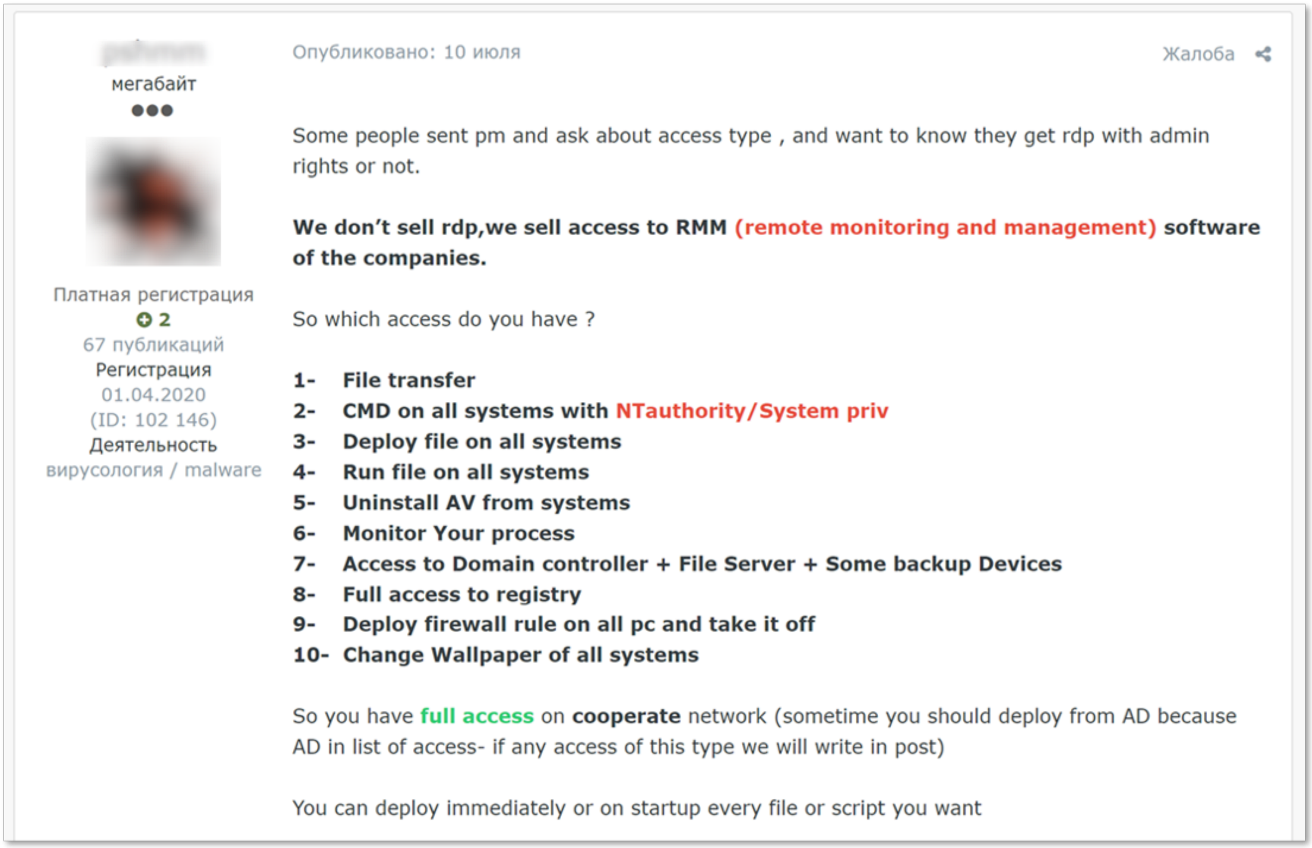
As can be seen, actors are binding together multiple vectors and technology stacks under the phrase “access” – from SQL injection to RDP access, everything goes. Not all network accesses are born equal, however: they vary in levels of sophistication needed to obtain the access, as well as in operations that can be performed by the actors after establishing persistence.

As such, **actors with different monetization TTPs may be interested in different access types.** For ransomware gangs, exfiltration of data and network-wide running of scripts is the goal – while for actors looking for PII, database access is king with endpoints being rendered useless. This is why some cloud-based applications, or credentials to third-party services, are a highly sought after commodity – while others may not be as interesting to actors.

Recently, **KELA has observed a case that is a perfect illustration of RMM access becoming a part of the RaaS (ransomware-as-a-service) ecosystem** – showcasing exactly why MSPs have become a prime target for actors.

Straight from the Horse’s Mouth

In September 2020, a threat actor posted 36 accesses for sale on a Russian-speaking underground forum. The new accesses are being sold for a cumulative price of $98,400 (in addition, for some accesses, the threat actor asked to suggest a price). Prior to this bunch of accesses, the actor was selling more than a dozen accesses in July, turning the total numbers to 53 accesses for a cumulative price of $153,850. So far, the actor managed to sell 10 accesses; they initially cost $33,800.



[redacted]
мегабайт
●●●

Платная регистрация
⊕ 2
67 публикаций
Регистрация
01.04.2020
(ID: 102 146)
Деятельность
вирусология / malware

Опубликовано: 10 июля

Жалоба

Some people sent pm and ask about access type , and want to know they get rdp with admin rights or not.

We don't sell rdp,we sell access to RMM (remote monitoring and management) software of the companies.

So which access do you have ?

1- File transfer
2- CMD on all systems with NTauthority/System priv
3- Deploy file on all systems
4- Run file on all systems
5- Uninstall AV from systems
6- Monitor Your process
7- Access to Domain controller + File Server + Some backup Devices
8- Full access to registry
9- Deploy firewall rule on all pc and take it off
10- Change Wallpaper of all systems

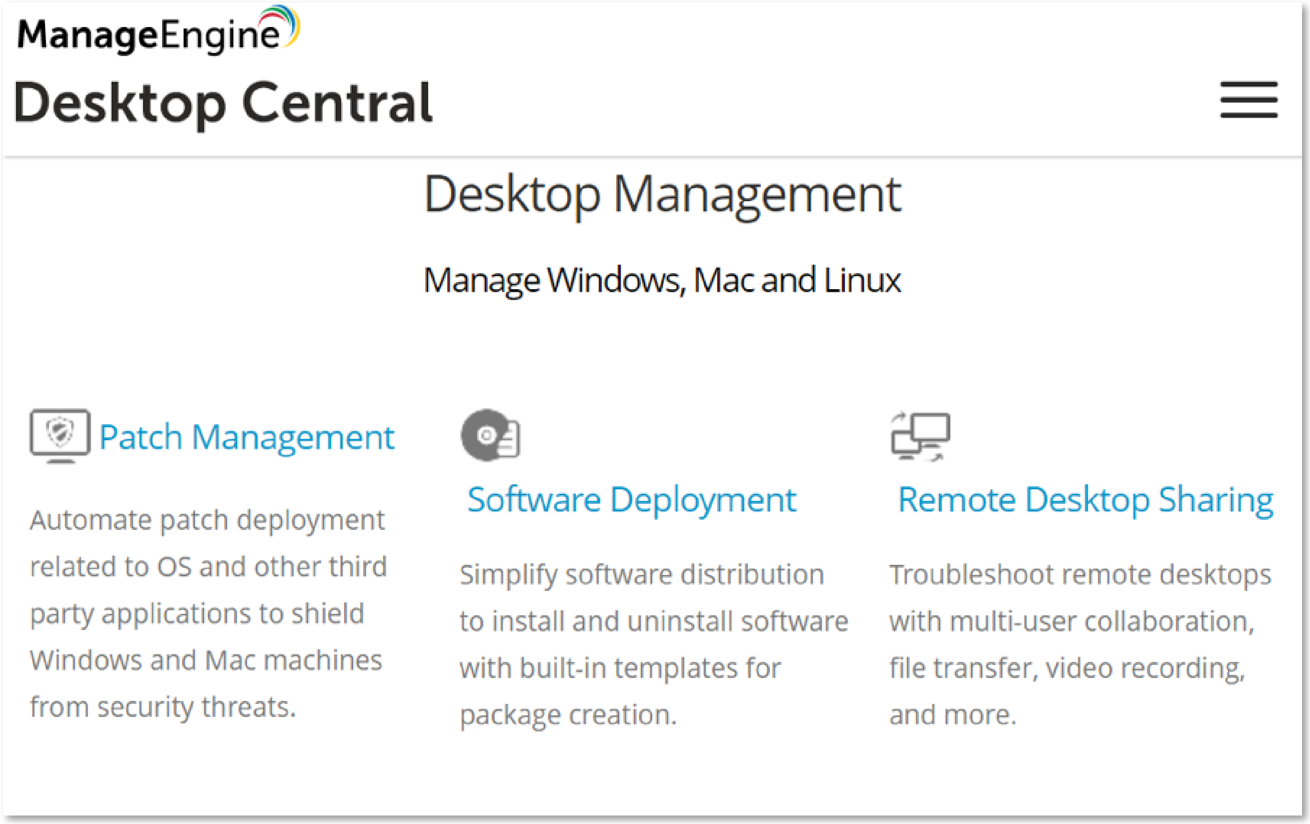
So you have **full access** on **cooperate** network (sometime you should deploy from AD because AD in list of access- if any access of this type we will write in post)

You can deploy immediately or on startup every file or script you want

Description of the type of access offered for sale

Based on KELA's analysis of multiple posts shared by the threat actor, **the targeted RMM software seems to be parts of the ManageEngine product suite developed by Zoho Corporation – and specifically Desktop Central** .

Examining some of Desktop Central's capabilities tells a pretty good story about why it would be attractive to threat actors – and particularly for ransomware gangs. It allows multiple operations to be carried out on the network, including remote control of hosts and – maybe most importantly – running custom scripts remotely on groups of endpoint devices.



ManageEngine

Desktop Central

Desktop Management

Manage Windows, Mac and Linux

Patch Management

Automate patch deployment related to OS and other third party applications to shield Windows and Mac machines from security threats.

Software Deployment

Simplify software distribution to install and uninstall software with built-in templates for package creation.

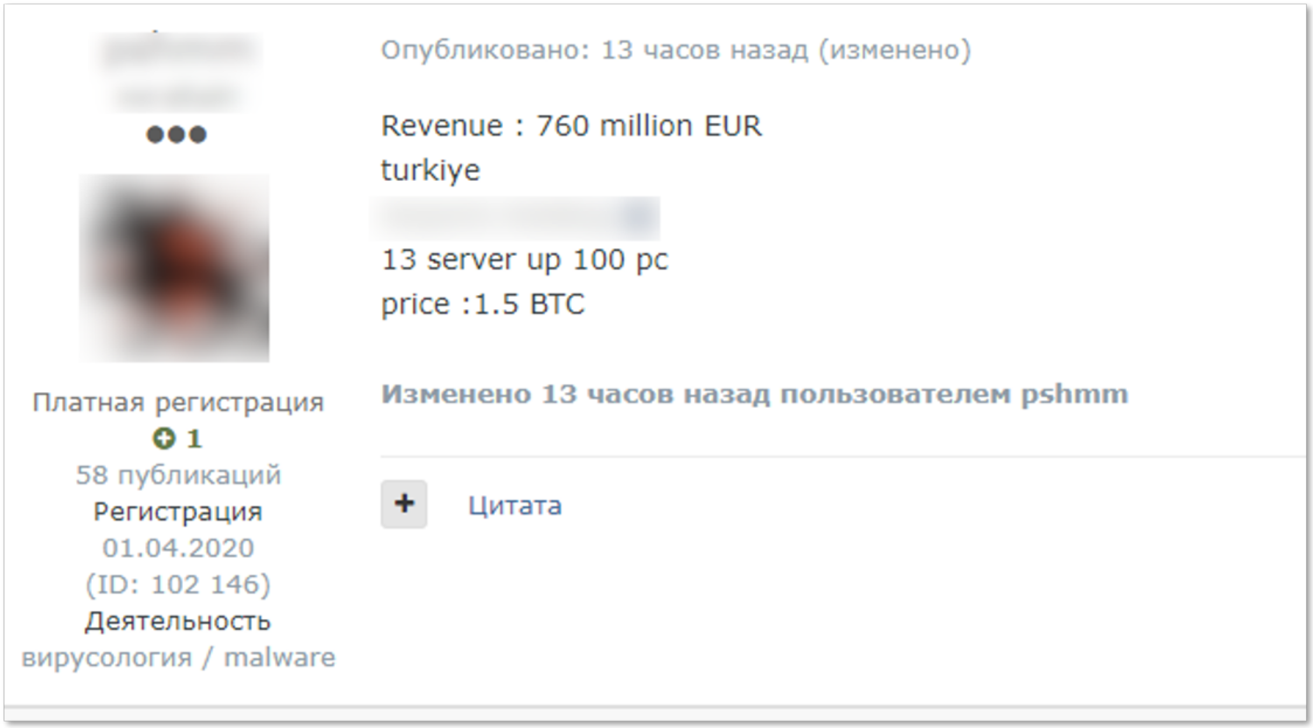
Remote Desktop Sharing

Troubleshoot remote desktops with multi-user collaboration, file transfer, video recording, and more.

A few of the Desktop Central features that may be attractive to ransomware actors (source: ManageEngine)

With multiple ransomware families depending on human-operated running of Powershell scripts, for example, it's easy to understand why RMM access would be appealing: it can allow for network-wide ransomware deployment without having to bypass any pesky Windows network protections, serving as a perfect living-off-the-land technique in the cloud.

In two cases with the most expensive accesses offered by the threat actor, KELA managed to identify the victims and indirectly confirm they were using the software in question. The first target is a Turkish company with a revenue of $221 Million (the access cost 1.5 BTC). The second victim is a Canadian corporation with a revenue of $338 Million, whose access has been sold in a few hours – it was offered for 1 BTC.



[redacted]

●●●

Платная регистрация

⊕ 1

58 публикаций

Регистрация

01.04.2020

(ID: 102 146)

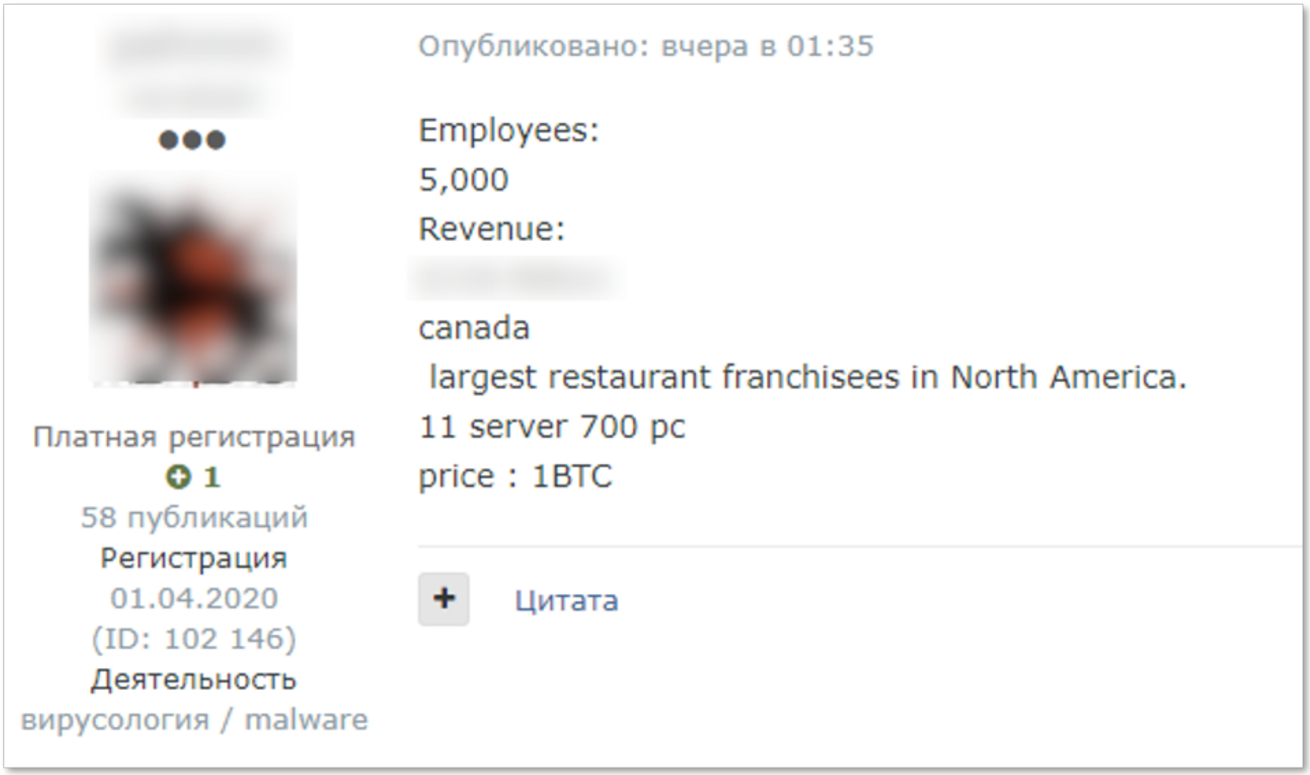
Деятельность

вирусология / malware

Опубликовано: 13 часов назад (изменено)

Revenue : 760 million EUR
turkiye
[redacted]
13 server up 100 pc
price :1.5 BTC

Изменено 13 часов назад пользователем pshmm



[redacted]

●●●

Платная регистрация

⊕ 1

58 публикаций

Регистрация

01.04.2020

(ID: 102 146)

Деятельность

вирусология / malware

Опубликовано: вчера в 01:35

Employees:
5,000
Revenue:
[redacted]
canada
largest restaurant franchisees in North America.
11 server 700 pc
price : 1BTC

But How?

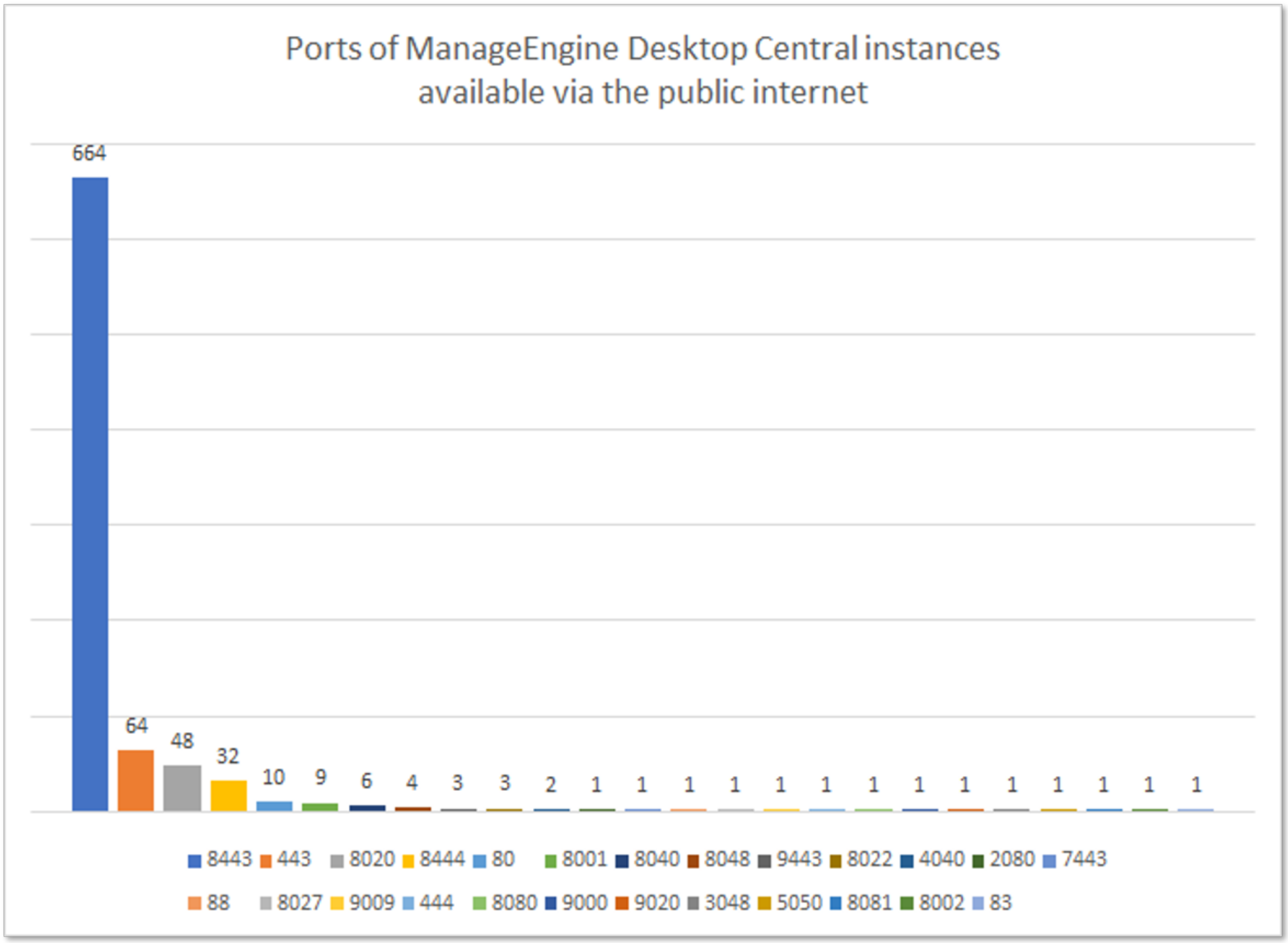
After establishing that Desktop Central seems to have been the vector to access obtained to over 30 organizations, the question is: how was the RMM compromised?

Generally speaking, two possible hypotheses exist:

1. An MSP hack: one (or more) MSP has been compromised, through which actors have obtained access to RMM software installed in the clients' environments – allowing direct network access;

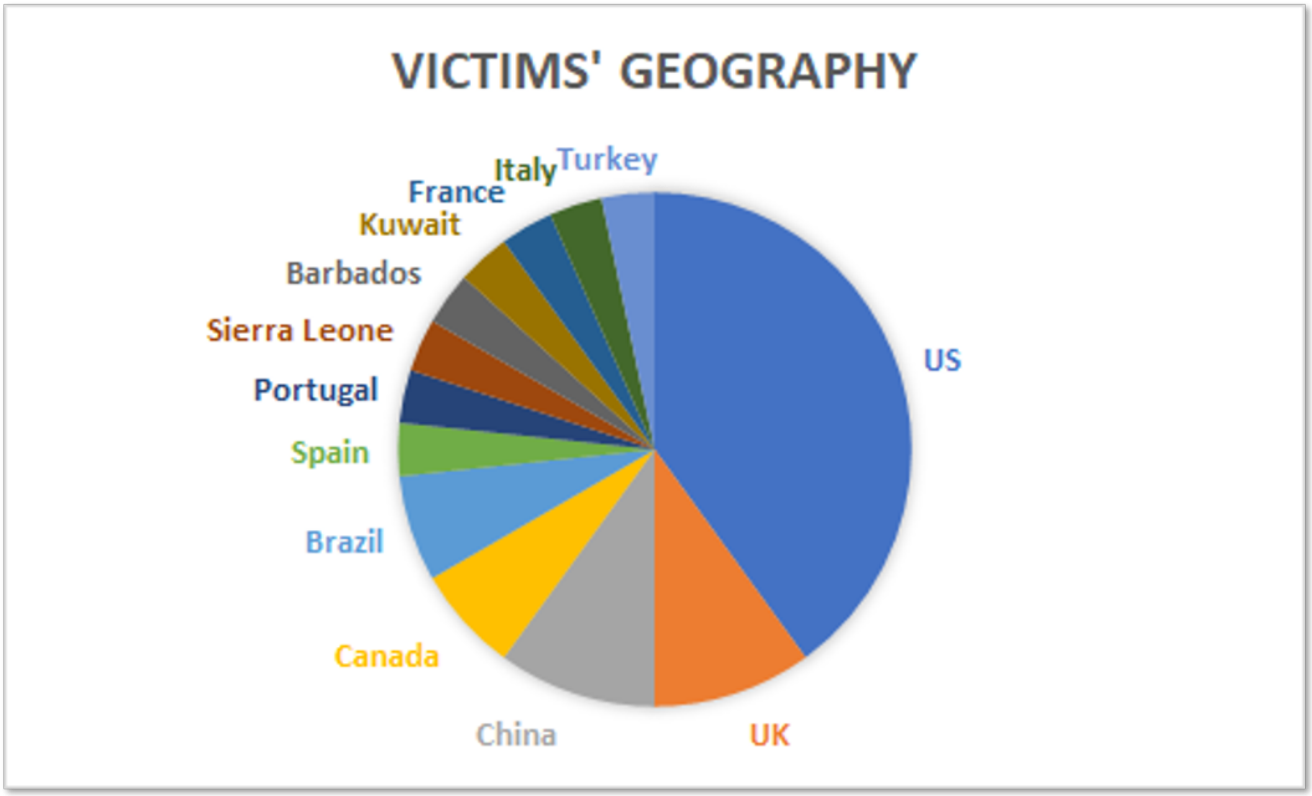
2. Direct targeting: organizations' Desktop Central instances were compromised directly – for example, via phishing, credentials harvesting or social engineering.

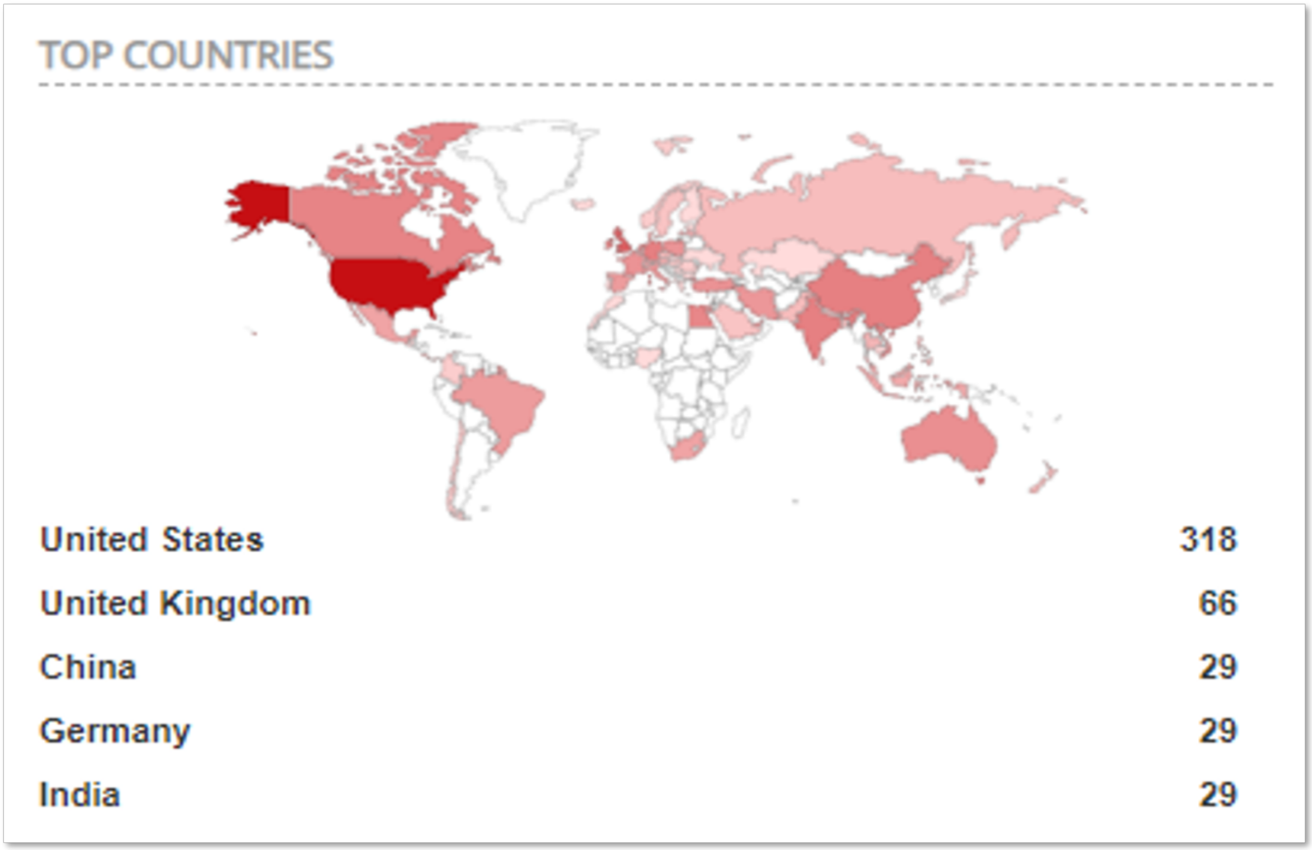
Trying to narrow down the options, KELA examined the prevalence of Desktop Central intances on the internet as reflected by Shodan. With almost 900 servers traced at the time of writing this blog, the RMM platform does seem to make a decent target – providing a wide net to cast for actors trying to obtain credentials for these cloud instances.



Examining the actors' victimology based on the data shared, **it appears that while most of the victims are US-based there's still a wide variety of targeted geographies**. The affected companies, as claimed by the actor, come from the US, the UK, Canada, Spain, Brazil, Portugal, and other countries. They include organizations from the IT, education, construction, manufacturing, law, healthcare, and other sectors. He also offered a couple of accesses related to the government organizations, specifically, in the U.S. (Arkansas state) and Barbados.

Intuitively speaking, **this may suggest that the centralized MSP hack is less plausible due to the geographic spread of victims** (unless, of course, more than one MSP was targeted), tilting the odds for direct targeting or exploitation.





TOP COUNTRIES

United States	318
United Kingdom	66
China	29
Germany	29
India	29

Top countries for Desktop Central instances available over the public internet, as seen on Shodan

---

This is not the first time Desktop Central is being targeted: a remote code execution vulnerability (CVE-2020-10189) was reported to have been exploited in attacks designed to drop malware in March 2020. While the vulnerability seems unrelated to the accessees discussed in this post (as they seem to employ legitimate credentials to access the software), it still showcases the interest in RMM software as a vector.

Update: October 8, 2020

Following this blog post and media exposure, the Zoho Corporation’s information security team proactively reached out to KELA in order to investigate the potential incidents. KELA was able to identify several victims as described in the threat actors’ RMM sales posts – and provided Zoho with the attributed victims; upon investigation, Zoho concluded that the identified victims seem to have utilized weak credentials to their ManageEngine products, which seems to be the root cause for the compromise. A potential hypothesis made early in the process, regarding the threat actor exploiting CVE-2020-10189 in order to create shadow accounts or persistent backdoors, was determined unlikely based on the victims investigated.

A response summarizing the investigation by the Zoho team reads:

With the current evidence, we strongly suspect that the usage of weak credentials is the cause of the attack, so we have:

1. Deployed live-changes that address the problem by preventing any future logins with the weak credentials.

2. Issued security guidance advisory to all our customers to help them ensure proper security measures are implemented in their installations.

KELA will continue to monitor the actors' activity and claimed victims in order to try and identify further TTPs used for the compromises. Whether the root cause is indeed weak credentials as concluded by Zoho, or may involve spear-phishing or other credential extraction methods, we recommend defenders to pay attention to the cloud attack surface expanded by internet-facing applications – as they sure do seem to attract bad actors.