



The Rise and Imminent Fall of the N-Day Exploit Market in the Cybercriminal Underground

Mayra Rosario Fuentes and Shiau-Jing Ding

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

Trend Micro Research

Written by

**Mayra Rosario Fuentes
Shiau-Jing Ding**

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963 – 2017)

<https://t.me/learningnets>

Contents

4

Introduction

7

Overview of Exploit Developers

12

Overview of Exploit Demand and Availability

16

Outdated Exploits

19

Exploit Subscription Services

21

The Future of the Exploit Market

23

Conclusion

The underground exploit market has undergone massive changes over the past few years. What used to be the sole domain of vendors of exploits for zero-day and N-day vulnerabilities has shifted toward alternative methods of monetization. (A zero-day vulnerability is a flaw, weakness, or bug in software or hardware that may have already been publicly disclosed but remains unpatched.¹ Once the vulnerability becomes public and the vendor or developer deploys a patch for it, it becomes a known or N-day vulnerability.)

The market for exploits used to be more lucrative. In recent years, we have seen a decline in advertisements on underground forums, possibly because sales have moved to exclusive locations or even the dark web. Furthermore, increased payouts from bug bounty programs make the underground market for N-day exploits scarcer, which, when combined with the market's volatility and a recent lack of trust with new vendors, makes for a changing exploit market.

Access-as-a-service has become the new hot commodity, providing a more lucrative alternative where vendors can demand higher prices than for N-day exploits and where there is less scrutiny from forum users. Many sellers who adopt this model specifically mention which exploits were used to compromise the victim entities. Access-as-a-service has the advantages of an exploit, but in its case all the hard work has already been done for the buyer. This results in greater demand for access-as-a-service vendors than for traditional exploit sellers, causing the N-day exploit market to shrink.

However, that is not to say that the zero-day and N-day exploit market is dead. Despite the competition, there is still heavy demand for exploits in the underground. Zero-day exploits still command high prices, while even N-day ones can still be peddled for lower sums. Even after a vulnerability is disclosed and patched, the exploit for it continues to be sold in underground marketplaces for months or even several years afterward.

On cybercriminal underground forums, users often post about exploits they would like to find or purchase. Based on our findings, exploits for Microsoft products were the most in-demand, an appetite that was in turn satisfied by sellers: at least 47% of requested exploits were for Microsoft products, while at least 51% of sales advertisements were for exploits for Microsoft products.

Based on underground forum listings, the typical price users were willing to pay for their requested N-day exploits was US\$2,000, while potential buyers were willing to pay over US\$10,000 for zero-day exploits. Although the cost for zero-day exploits can reach thousands of dollars, cybercriminals can find bargain prices for N-day exploits — such as JavaScript exploits for US\$40 and Microsoft Word exploits for US\$100 — or even the occasional free exploits shared on English-language underground forums. It is worth noting that prices on Russian-language underground forums are usually higher than on English-language ones.

Vulnerabilities and, by extension, exploits can have long life expectancies — even over 10 years in some cases. While 54% of exploits sold in the underground were released during the past two years, the oldest exploit we found that was being sold in the cybercriminal underground was one for a vulnerability disclosed in 2012.

This research covers the cybercriminal underground market of N-day exploits. It is based on a study we conducted over two years, from January 2019 to December 2020. It explores the life cycle of an exploit on cybercriminal underground forums, beginning with the initial sales discussions among malicious actors and proceeding to the use of the exploit through infections until end of life.

Introduction

The typical life cycle of an exploit in the underground often goes as follows:

1. A developer presents a proof of concept for an exploit or creates a working exploit.
2. Malicious actors or governments weaponize the exploit, keeping it secret if necessary (in the case of governments).
3. Sellers offer the exploit in the cybercriminal underground.
4. A security researcher or a participant in a bug bounty program discovers the vulnerability being exploited.
5. The affected vendor becomes aware of the vulnerability.
6. The affected vendor creates and releases a patch for the vulnerability.
7. Cybercriminals either:
 - Continue selling the “patched” exploit for at least 2 years at a lower price, often bundling it with other dated exploits to gain more profits.
 - Stop selling the exploit.

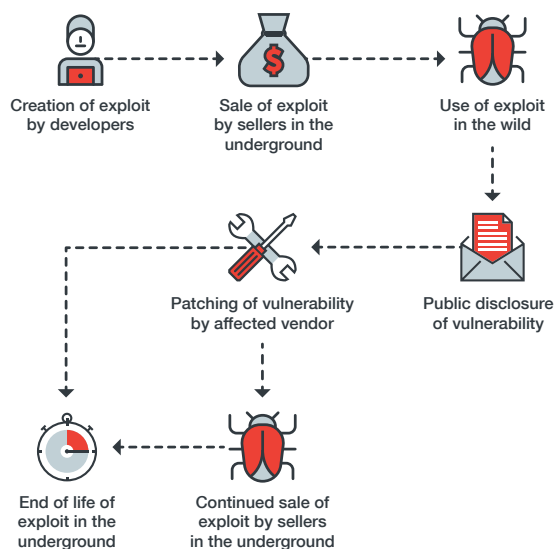


Figure 1. The typical life cycle of an exploit in the underground

As an example, the life cycle of an exploit for CVE-2020-9054, which has been peddled since at least February 2020, is shown in Figure 2. This vulnerability could allow remote code execution (RCE) in affected Zyxel network-attached storage (NAS) products. The timeline shows how the exploit depreciated in price from US\$20,000 to US\$2,000 in just 6 months.



Figure 2. The life cycle of an exploit for the Zyxel NAS vulnerability CVE-2020-9054^{2, 3}

Patching and tracking updates have become a daunting task for administrators and IT teams, especially since these are only a small part of the everyday tasks of an often already thinly distributed team.⁴ An average organization, for instance, reportedly takes around 50 days to patch a critical vulnerability in one of its applications.⁵ Testing whether the patch works while not disrupting business operations can also be challenging.

2020 saw more security vulnerabilities disclosed than any other year to date, with about 50 CVE (Common Vulnerabilities and Exposures) ID numbers per day. Given the increasing number of vulnerabilities disclosed per year, there is a need for organizations to find effective ways to determine which vulnerabilities to prioritize, especially since, according to the National Institute of Standards and Technology, 68% of all vulnerabilities reported in 2020 required no user interaction of any kind for them to be exploited.⁶

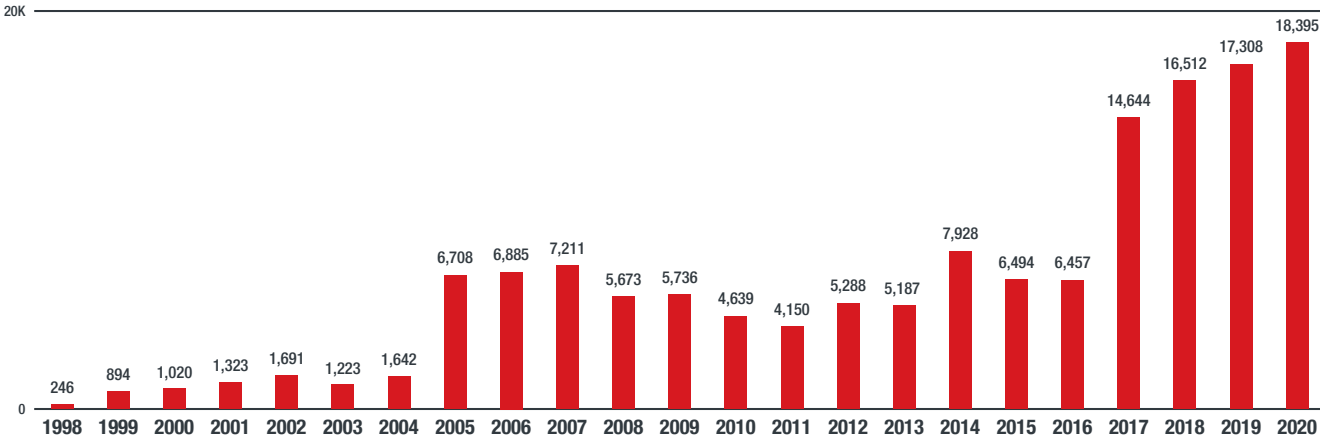


Figure 3. The number of published software vulnerabilities per year based on assigned CVE ID numbers⁷

5 | The Rise and Imminent Fall of the N-Day Exploit Market in the Cybercriminal Underground

When analyzing the potential risk that vulnerabilities pose, organizations must consider more than just the severity scores; they should also look at what cybercriminals are looking to exploit in the underground. Many vulnerabilities are never or rarely exploited in the real world because they are too complex or require malicious actors to have access to high-level privileges. In underground marketplaces, cybercriminals often sell exploits that are easy to use, such as Microsoft Word exploits that can be used with phishing attacks or similar exploits that require low user interaction.

For example, many machines have been targeted with the exploit for CVE-2017-8543, which affects the Microsoft Windows Server Message Block (SMB) service and is used by the WannaCry ransomware. The exploit is still being actively used, as evidenced by Trend Micro's detections of variants of the original WannaCry code in 2020⁸ and 2021. What keeps WannaCry prevalent is not only the spreading power of self-propagating malware but also the longevity that such a successful exploit could have in the wild before patch levels make an impact on its spread. This same longevity is the key enabler for the entire N-day exploit market.

Overview of Exploit Developers

Over the past two calendar years, we used the “XSS” and “Exploit” tags to investigate a handful of participants on cybercriminal underground forums who had been in the business of selling exploits for several years and who had been specializing in zero-day and N-day offerings. These forums can be quite difficult to penetrate for new sellers trying to enter the exploit business as they are usually heavily scrutinized, with forum users asking how they could demand high prices without having a good reputation or with minimal forum activity. Often, sellers on these forums will not attempt to sell another exploit if they get an unwelcome reception. Many of the most experienced sellers earn their reputation over several years, making their name not only by offering zero-day and N-day exploits, but also by buying them — further making this market a tough one to break into.

We came across a new exploit developer on the forum Hack Forums who attempted to sell a zero-day PDF exploit builder for US\$950 in September 2020. The seller was questioned for having been on Hack Forums for only a month. Furthermore, there was disbelief among users since a true zero-day exploit would demand between US\$5,000 and US\$10,000. This user is currently no longer registered on Hack Forums.

Once an exploit has been out for several weeks or months, its price is discounted. For example, an N-day exploit for the kernel local privilege escalation vulnerability CVE-2018-8453 was advertised for sale in December 2018 for US\$10,000 on the forum Exploit. By February 2019, the price had been discounted to US\$5,000. Another example was an N-day exploit for uploading a web shell to Magento 2 that was advertised in November 2019 for US\$10,000 on the same forum. The price was lowered to US\$8,000 a month later and to US\$7,000 about 2 months later. Yet another example was the Zyxel zero-day exploit mentioned in the previous section. Zyxel released a patch about 2 weeks later, after which a different actor peddled the exploit for US\$10,000.

16.05.2020

ZyXEL NAS pre-auth RCE via OS Command Injection
 Цена: \$10,000
 Описание:

1. Item name : ZyXEL NAS pre-auth RCE via OS Command Injection
 1. Affected OS: NAS Vulnerable Firmware Version: Firmware Release V5.21(AAZF.5)C0 (latest) and all precedent releases
 NAS Vulnerable Models: NAS542, NAS540, NAS520, NAS325, NSA325 v2, NSA325, NSA320S, NSA320, NSA310S, NSA310, NSA221, NSA220+, NSA220, NSA2107
 Vulnerability can also be tweaked to exploit: Firewall Vulnerable Firmware Version: UTM, ATP, and VPN firewalls running firmware version ZLD V4.35 Patch 0 through ZLD V4.35 Patch 2. Those with firmware versions before ZLD V4.35 Patch 0 are NOT affected.
 Firewall Vulnerable Models: ATP200, ATP500, ATP800, USG20-VPN, USG20W-VPN, USG40, USG40W, USG60, USG60W, USG110, USG210, USG310, USG1100, USG1900, USG2200, VPN50, VPN100, VPN300, VPN1000, ZyWALL110, ZyWALL310, ZyWALL1100

2. Vulnerable Target application versions and reliability.
 List complete point release range. see previous ranges

3. Tested, functional against target application versions, list complete point release range.
 see previous ranges

Нажмите, чтобы раскрыть...

Упомянутый в Krebs on Security:
<https://krebsonsecurity.com/2020/02/zyxel-fixes-0day-in-network-storage-devices/>
<https://krebsonsecurity.com/2020/02/zyxel-0day-affects-its-firewall-products-too/>

Firewall Vulnerable Models

- ATP200, ATP500, ATP800, USG20-VPN, USG20W-VPN, USG40, USG40W, USG60, USG60W, USG110, USG210, USG310, USG1100, USG1900, USG2200, VPN50, VPN100, VPN300, VPN1000, ZyWALL110, ZyWALL310, ZyWALL1100

NAS Vulnerable Firmware Version

- Firmware Release V5.21(AAZF.5)C0 (latest) and all precedent releases

Figure 4. A forum post advertising a “discounted” Zyxel exploit for US\$10,000

14.05.2020

CVE 2020-0674 Is IE vulnerability patched in 2020 Feb. MS Office Addins use default browser IE or edge only no matter what other browsers are installed on computer. This exploit will work with MS office on below mentioned computers

Код: Скопировать в буфер обмена

```

Windows 7 x86 Yes
Windows 8 x86 Yes
Windows 8.1 x86 Yes
Windows 10 x86 ver. > = 1903 Yes
Windows 7 x64 Yes
Windows 8 x64 Yes
Windows 8.1 x64 Yes

Windows 10 ver. <1903 / Office 365
Windows 10 ver. > = 1903 / Office 365 ver <16.0.116291

Office 2007 to office 365 ver <16.0.11629 yes [/ CODE]

[CODE] REF :: https://docs.microsoft.com/en-us/office/dev/add-ins/concepts/browsers-used-by-office-web-add-ins

```

Price 25k USD, payment in BTC.

Escrow deal is welcome, you pay the fee.

Runtime bypass on AVG, Avast, Kasper, McAfee, Windows Defender, ESET, Avira (Other AV can check on demand)

Scantime:

Figure 5. A forum post advertising an Internet Explorer exploit for US\$25,000

06/05/2019

User
 (L1) cache
 check in: 04/29/2008
 Posts: 516
 Reactions: 428

Gentlemen, developers and brokers!
 - I constantly buy various 0day / Nday.
 - I have finances, I check the goods quickly.
 - Complete anonymity and confidentiality.
 - I work strictly through a guarantor.
 - No prepayment.
 - The guarantor at my expense.

In some cases, it is possible to exchange your 0day for the 0day I have, or sell mine.
 The first contact via PM, then only jabber + otr.

05/13/2020

Vulnerability Broker
 Premium
 check in: 01/17/2019
 Posts: fourteen
 Reactions: one

Sell 0day exploit for Internet Explorer
 Punches
 OC: Windows 7, 8.1, 10.
 Windows Server 2008, 2012, 2016
 Internet Explorer 8, 9, 10, 11.
 Price - \$ 100k

Deal only strictly through the guarantor at your expense.

I am starting to sell FUD WinRAR 1 day exploit [CVE-2018-20250]. You can see details under below:

How to Work: When user extract the files in RAR, target file will be written in Windows startup folder and after reboot, it will be run automatically by Windows.

WinRAR does not have auto-updates so it means, if you have old WinRAR version, you don't see auto-update screen or something. You need to delete your old WinRAR and download latest WinRAR, but everyone knows, no-one do that. 😞

This means many users don't use latest WinRAR version.

Vulnerability: CVE-2018-20250 Affected Versions: <WinRAR 5.70 [Latest WinRAR version] Supported architecture: x86 / x64 Scan Result: <https://avcheck.net/id/G00uZVGRUZA6> POC: <https://www.youtube.com/watch?v=R2qcBWJzHMo> More Details: <https://www.tenable.com/blog/winrar-absolute-path-traversal-vulnerability-leads-to-remote-code-execution-cve-2018-20250-0>

PS: You can add every file types in RAR file, [.jpg, .png, .txt, etc ..] and your .exe file does not appear in RAR.

Contact: PM

Published by 12 August, 2019

win lpe without 10k (raising rights) - \$ 100k (to get out of the sand acrobat, etc.)
 acrobat pdf - 130k \$
 only a guarantor, not a lot of bargaining is possible
 write only to those who really want to buy and can
 work under% is not interesting

Looking to sell my Microsoft office 0day Exploit

08-20-2020, 09:53 AM

[newb@HF]
 Posts: 26
 Threads: 4
 B Rating: 0
 Popularity: 39
 Bytes: 37.65
 Game XP: 0

RCE exploit type of vulnerabilities is Heap-Based Memory Corruption due to Malformed TTF Font the payload and pdf get loaded into the heap and EIP somehow gets its value to point into that heap area
 this only real adobe expl that exist and it bypass adobe sandbox as well
 when u ready can provide TV or anydesk demo

video demo : [redacted]

only 2 copies

Start Contract

Figure 6. Examples of forum posts by exploit developers. The second one is asking for a high price but has a good reputation.

Forum users often discuss legitimate bug bounty programs in a positive way. On some English-language forums, we encountered users posting how-to guides and tips on how to submit exploits to bug bounty programs. We also saw a leaked SANS Institute course on bug bounties and responsible disclosure being shared for free.⁹

However, forum users also complain about bug bounty programs. Their complaints include long wait times for replies, maxing out the allowed number of submissions, and issues with payments. For some exploit developers, these and other shortcomings of bug bounty programs are enough reason for them to sell their exploits in the cybercriminal underground rather than submitting their exploits to bug bounty programs.

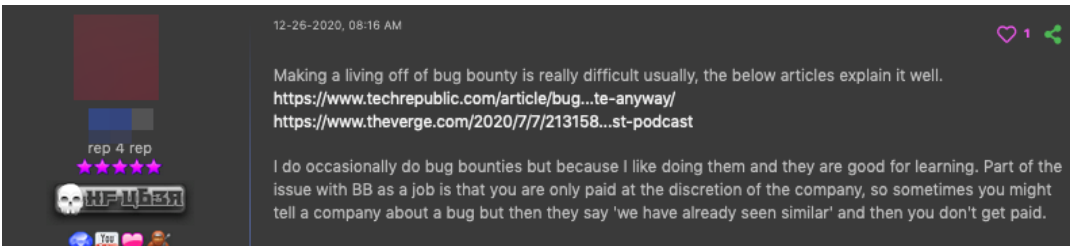


Figure 7. A forum post about bug bounty programs

A small group of disgruntled bug bounty hunters use the underground to sell their exploits and sometimes even offer their coding skills as well. For example, we saw a user on Hack Forums who provided a snapshot of their bug bounty program submissions, offered their coding services, and looked for potential buyers of their exploits. Another example was a user on RaidForums who decided to sell their exploits for cybercriminal use instead of submitting them to a bug bounty program.

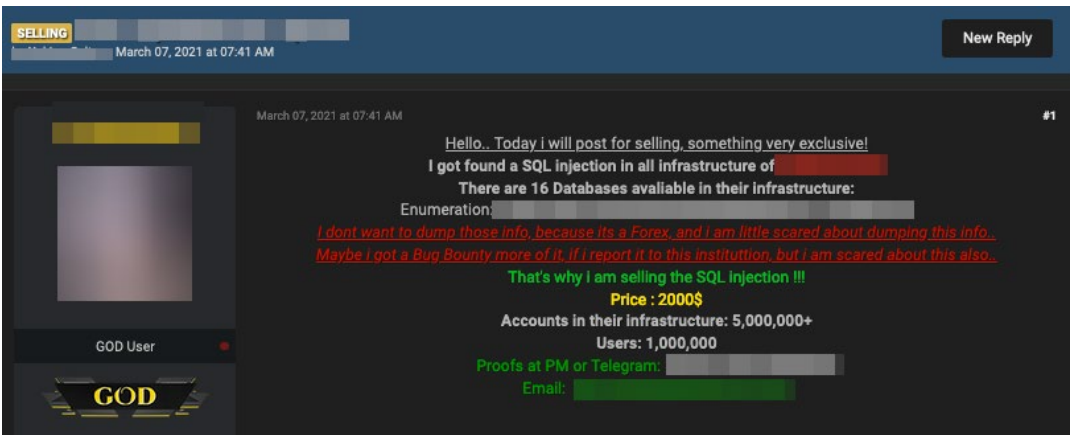


Figure 8. A post on RaidForums by a user selling access to their exploits

Some opportunistic users advertise themselves as “private companies” looking to buy zero-day exploits from sellers. These users submit the exploits to bug bounty programs, sell them to cybercriminals, or are just looking for exploits for themselves. Some advertisements we saw were from users who actively

submitted exploits to bug bounty programs. Others were from users who were looking to trade with other forum users who might not have the knowledge or experience in determining how much their exploits could be sold for to bug bounty programs. We saw advertisements, for example, that requested functional prototypes of exploit code and the sort of detailed technical description that would also be required by a bug bounty program.

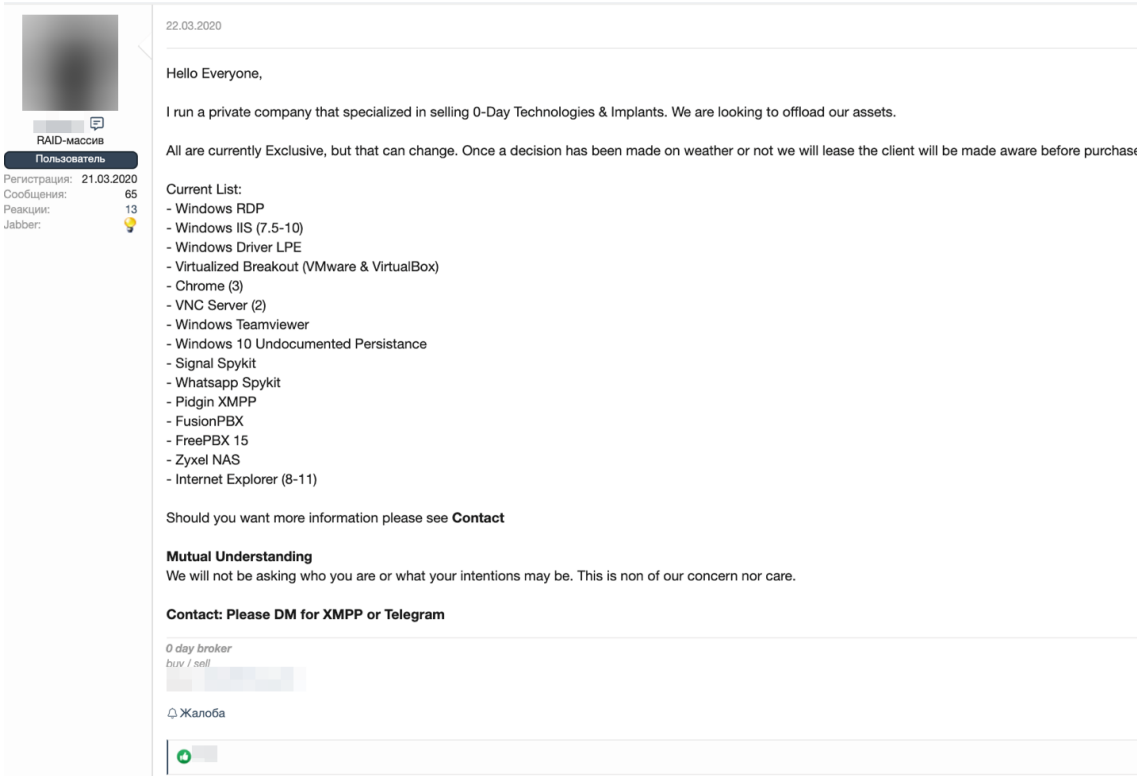


Figure 9. A forum post by a “private company” advertising their interest in purchasing zero-day exploits

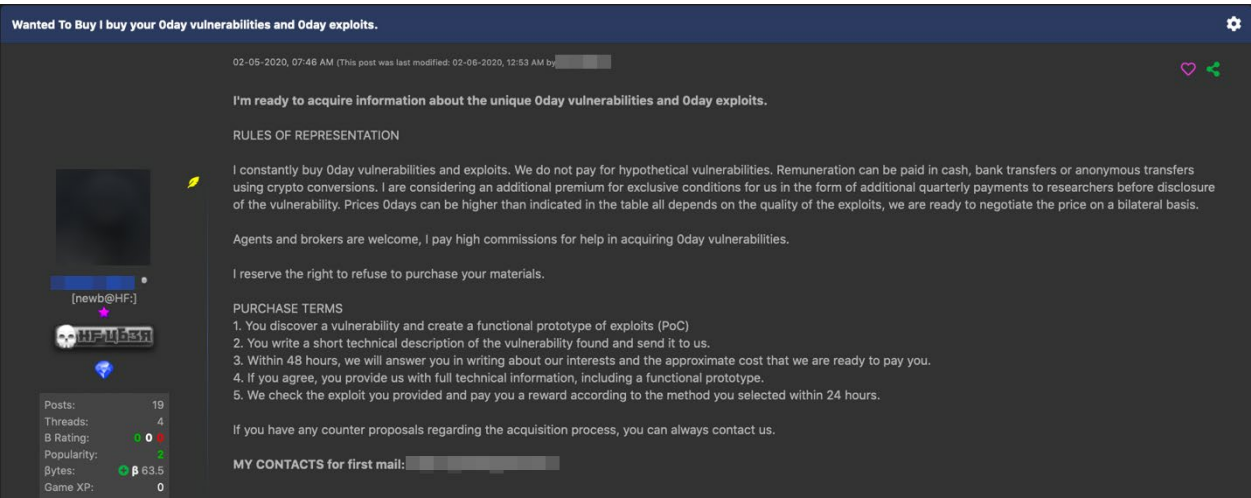


Figure 10. A forum post by a zero-day exploit buyer looking for the sort of documentation a bug bounty program would require

Overview of Exploit Demand and Availability

We researched advertisements for exploits for sale, filtering out those that looked like they were from scammers or from actors who had a low reputation. We also looked at what users were requesting to purchase, that is, their wish list of exploits for certain vulnerabilities.

Exploits for Microsoft products were the most requested in the cybercriminal underground, with Microsoft Office, Microsoft Windows, Microsoft Remote Desktop Protocol (RDP), Internet Explorer, and Microsoft SharePoint accounting for a total of 47% of requested exploits. While exploits for internet-of-things (IoT) devices made up only 5% of requests, we expect IoT devices to become more lucrative targets for malicious actors because of the ever-increasing number of connected devices and because many IoT devices are not easily patchable (or not patched at all).



Figure 11. The distribution of affected products in exploits requested by users on cybercriminal underground forums

Most of the exploits advertised on cybercriminal underground forums were for Microsoft products: Microsoft Office, Microsoft Windows, Microsoft RDP, Internet Explorer, and Microsoft SharePoint had a combined market share of 51%.

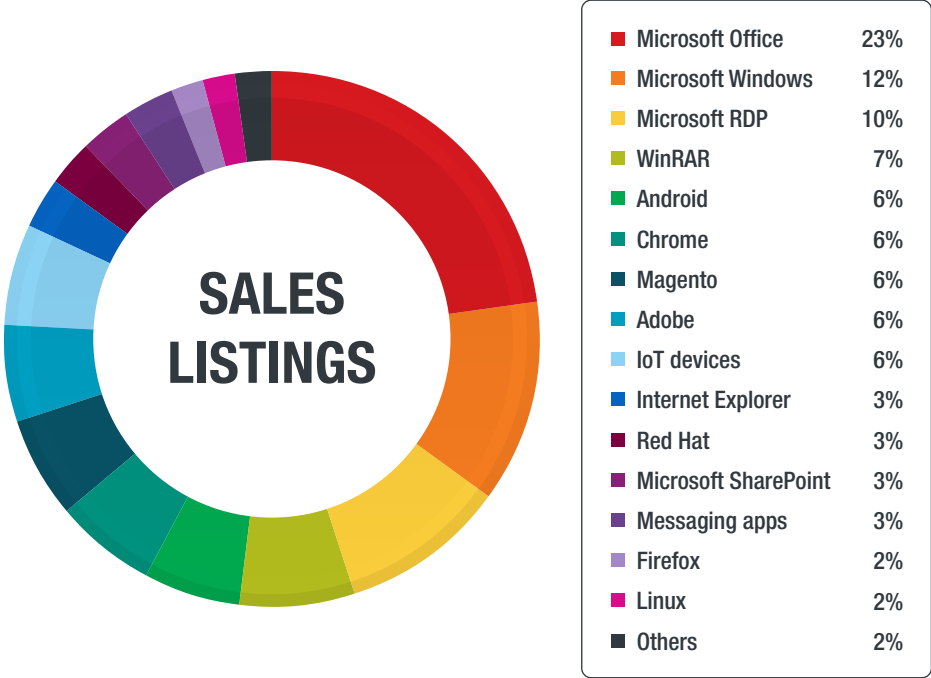


Figure 12. The distribution of affected products in exploits sold by users on cybercriminal underground forums

The average price users were willing to pay for exploits was US\$2,000. But we found some affordable exploits for sale, particularly on Russian-language forums, including ones for Microsoft RDP (as low as US\$200), WinRAR (US\$200), and Cisco (US\$1,000). On English-language forums, prices started even lower, with some Microsoft Word and Excel exploits going for as low as US\$35.

Affected product	Price
Microsoft Office	US\$35 – US\$500,000
Microsoft RDP	US\$200 and up
WinRAR	US\$200 – US\$10,000
PDF	US\$250 and up
Microsoft Windows	US\$500 – US\$10,000
Cisco	US\$1,000 and up
Internet Explorer	Up to US\$25,000

Table 1. The typical prices for N-day exploits, for commonly affected products, sold on cybercriminal underground forums

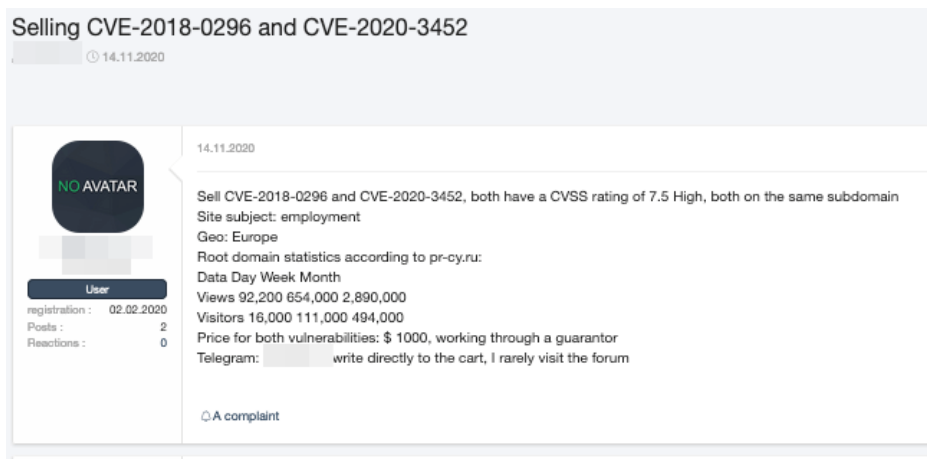


Figure 13. A post on a Russian-language forum advertising Cisco exploits for US\$1,000

Russian-language forums also had a greater variety of exploits for sale (unlike English-language forums, where the most commonly advertised exploits were for Microsoft Office and Adobe Acrobat Reader), with silent exploits being the most popular. Silent exploits are designed to run silently in the background when the file containing the exploit is opened and to automatically install the malware unbeknown to the victim. Ideally, they are completely undetectable at runtime and to antimalware.

We also looked into how the wish list of users compared with the actual sales listings for exploits for Microsoft products on cybercriminal underground forums. We noticed that what was requested was more or less similar to what was offered — the supply adapted to what the consumers were demanding.

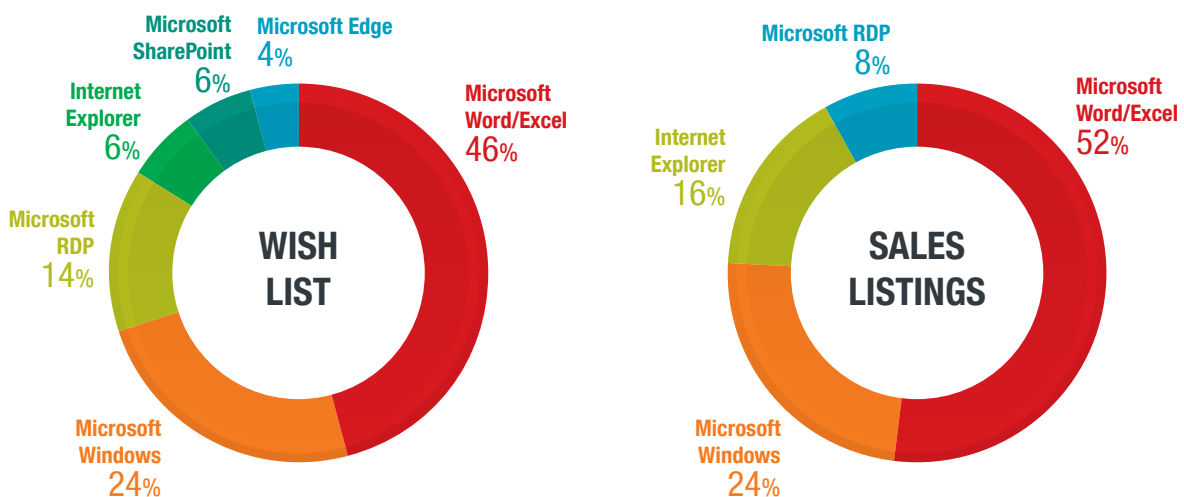


Figure 14. A comparison of exploits for Microsoft products requested and sold by users on cybercriminal underground forums

Naturally, the demand for and availability of exploits are high while they are relatively new or recent. Just under half of exploits requested and just over half of exploits sold by users on cybercriminal underground forums were for vulnerabilities that were disclosed in 2019 and 2020. Most of the N-day exploits advertised on English-language forums were from 2017 or 2018, while those advertised on Russian-language forums were mostly a year old.

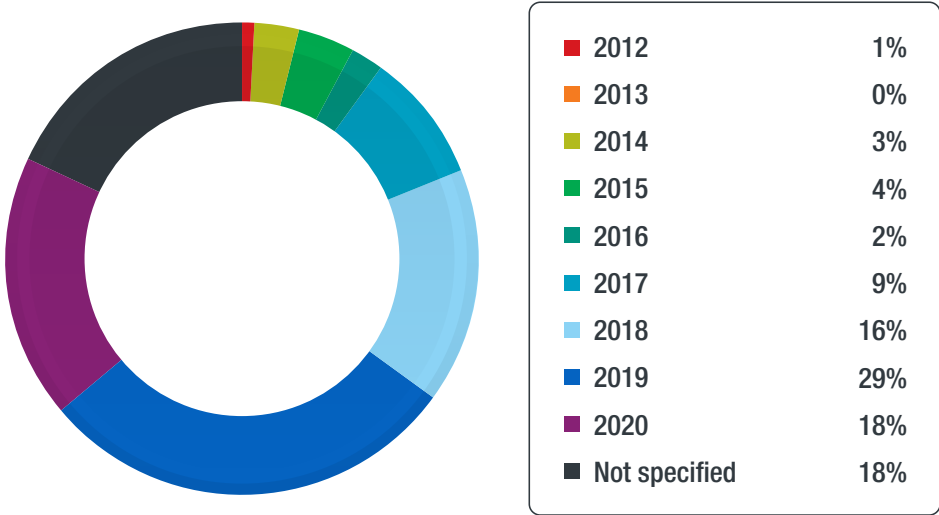


Figure 15. The distribution of exploits requested by users on cybercriminal underground forums based on the years of disclosure of the vulnerabilities they are for

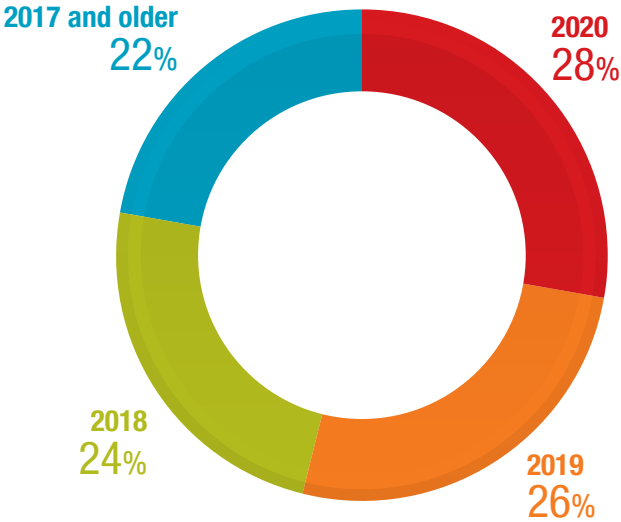


Figure 16. The distribution of exploits sold by users on cybercriminal underground forums based on the years of disclosure of the vulnerabilities they are for

Outdated Exploits

Just because an exploit is outdated does not mean it is useless. In fact, exploits for some of the oldest vulnerabilities continue to be sold. Cybercriminals want to use the cheapest tool to get their job done, which, in most cases, does not require a zero-day or recently discovered vulnerability. As a result, they turn to more dated vulnerabilities, including decade-old ones. Exploits for vulnerabilities that have been patched for years go for cheap in the underground. Especially on English-language forums, users requested old exploits or asked for help with implementing outdated exploits.

For example, variants of the original WannaCry ransomware are still prevalent today. WannaCry relies on EternalBlue, an exploit for CVE-2017-0144. Microsoft had already released the patch for the vulnerability through its MS17-010 security bulletin about two months before the initial outbreak of the ransomware in May 2017. Given that the vulnerability had been patched, the outbreak should not have affected many endpoints in the first place. However, because of various factors, many organizations failed to apply the patch — and many continue not to do so. In fact, as noted in Trend Micro’s annual cybersecurity report, WannaCry was the most detected malware family in 2020.¹⁰ And according to Shodan, as of June 2021, there are still more than 650,000 devices vulnerable to WannaCry.

In 2020, we looked into an actor who sold exploits for versions of Microsoft Excel from 2007, a version of Internet Explorer from 2013, and older versions of Microsoft Windows 10 for US\$15 each on a Russian-language forum. The actor often bundled these exploits together so that the convenience of buying all at once could command a higher price. On an English-language forum, another actor sold a bundle of exploits, with the oldest affected vulnerability originating from 2010, for US\$800. Some actors also included virus scanner results to demand higher prices for their exploits.

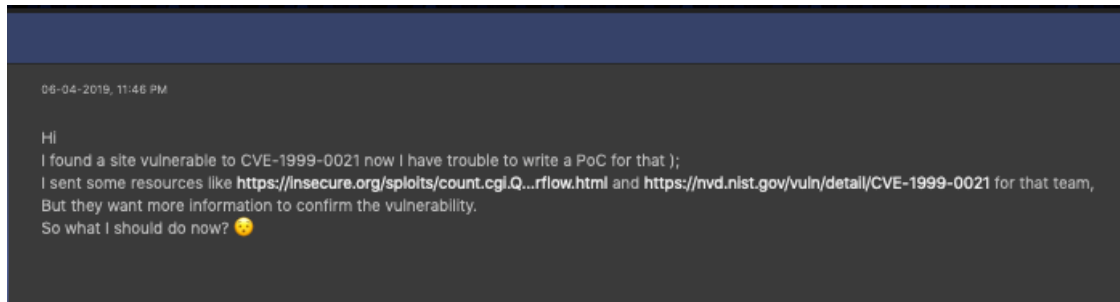


Figure 17. An English-language forum user requesting help on how to exploit CVE-1999-0021 in 2019 after discovering an unpatched website, 20 years after the disclosure of the vulnerability

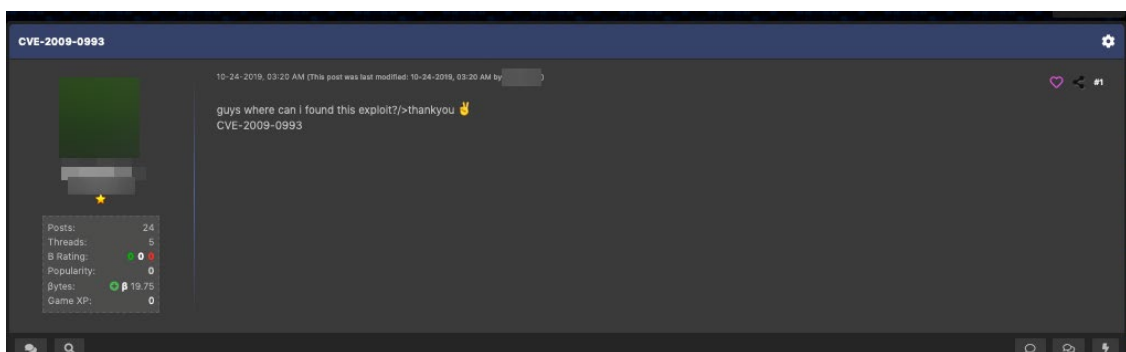


Figure 18. An English-language forum user asking for information about an exploit for an 11-year-old vulnerability

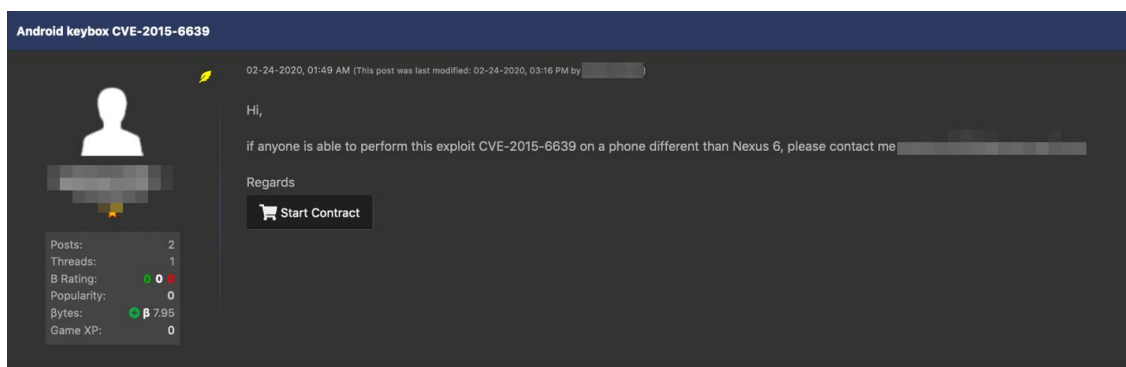


Figure 19. An English-language forum user asking for information about an exploit for an Android vulnerability from 2015

One of the oldest vulnerabilities we found for which an exploit was being sold was CVE-2016-5195, a kernel vulnerability that could allow any unprivileged existing user to escalate their privilege to root. It is also known as Dirty COW, after copy-on-write (COW), a technique used by Linux to reduce duplication of memory objects. As shown in Figure 20, an exploit for Dirty COW still managed to fetch US\$3,000 over 2 years after the disclosure of the vulnerability.

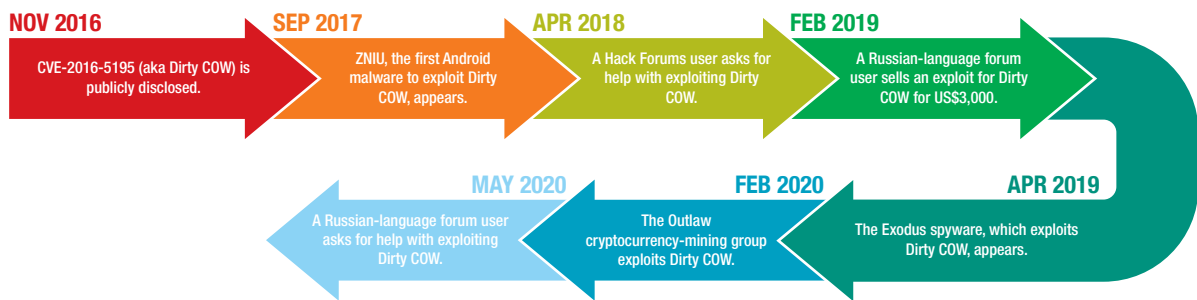


Figure 20. How CVE-2016-5195 (aka Dirty COW) was exploited over the years^{11, 12, 13}

In addition to older exploits being sold, there were occasional outdated exploits shared for free on both English- and Russian-language forums.

Exploit Subscription Services

Some cybercriminals offer exploit tools for a monthly fee, ranging from US\$60 to US\$2,000. Some of the subscription services they offer include exploits that are outdated; by bundling these exploits, they can demand a higher price.

One seller we found offered a monthly subscription to an exploit builder starting at US\$60. The service boasted multiple exploit categories — including Microsoft Word, Microsoft Excel, and JavaScript exploits — and guaranteed that the exploits were “FUD” (fully undetectable) and would be updated weekly. A subscriber could pick which exploits to use for the file that they wished to weaponize.

Another seller offered an exploit builder bundling exploits for CVE-2017-11882, CVE-2017-8570, and CVE-2018-0802, for US\$1,150 a month, with similar guarantees for fully undetectable runtime and monthly updates. This exploit builder bundled all three exploits into a Microsoft Word document instead of allowing a subscriber to choose which exploits to use.

These subscription services provide quick access to less sophisticated users as most of the work is already automated for them, lowering the barrier for entry to cybercrime. Customers appear to be satisfied with the services, but they do not seem to be aware of what the sellers of the services are doing to be able to keep the exploits undetectable every month.

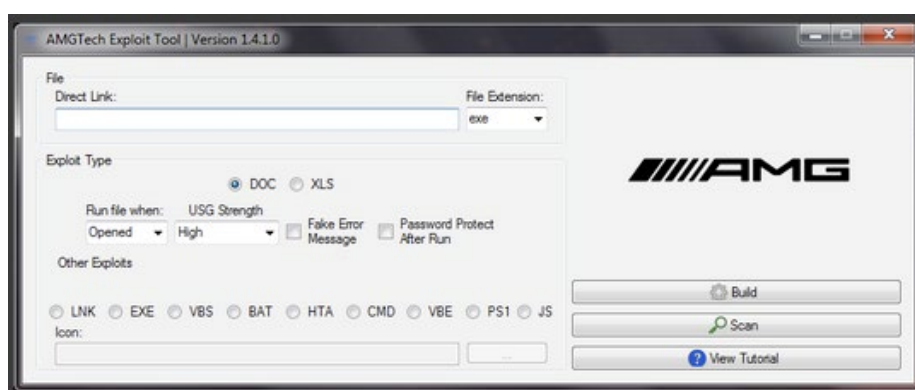


Figure 21. An exploit builder tool offered as part of a subscription service

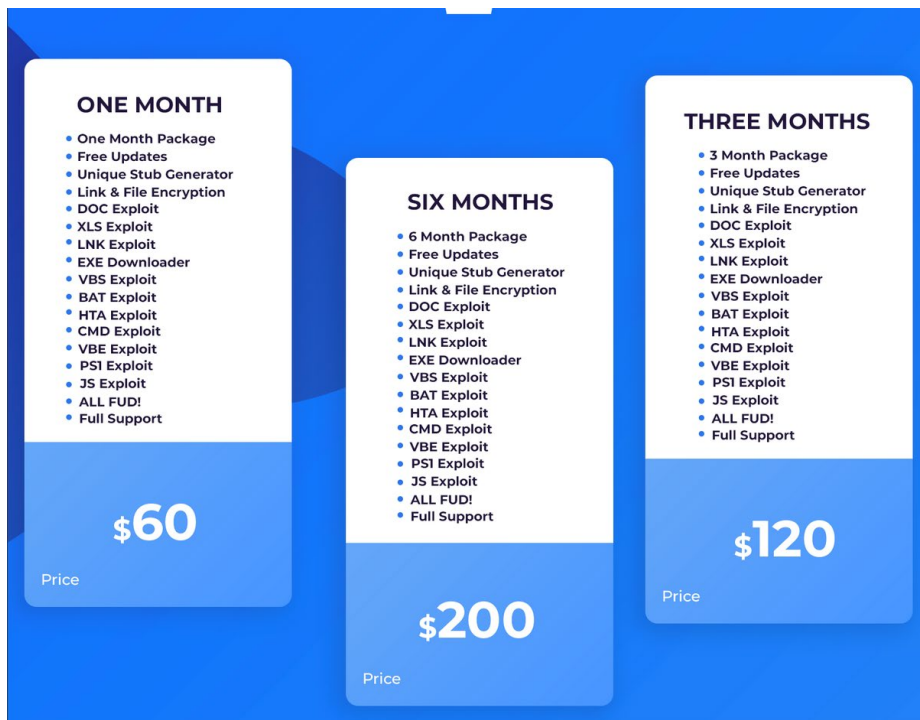


Figure 22. The pricing for an exploit subscription service

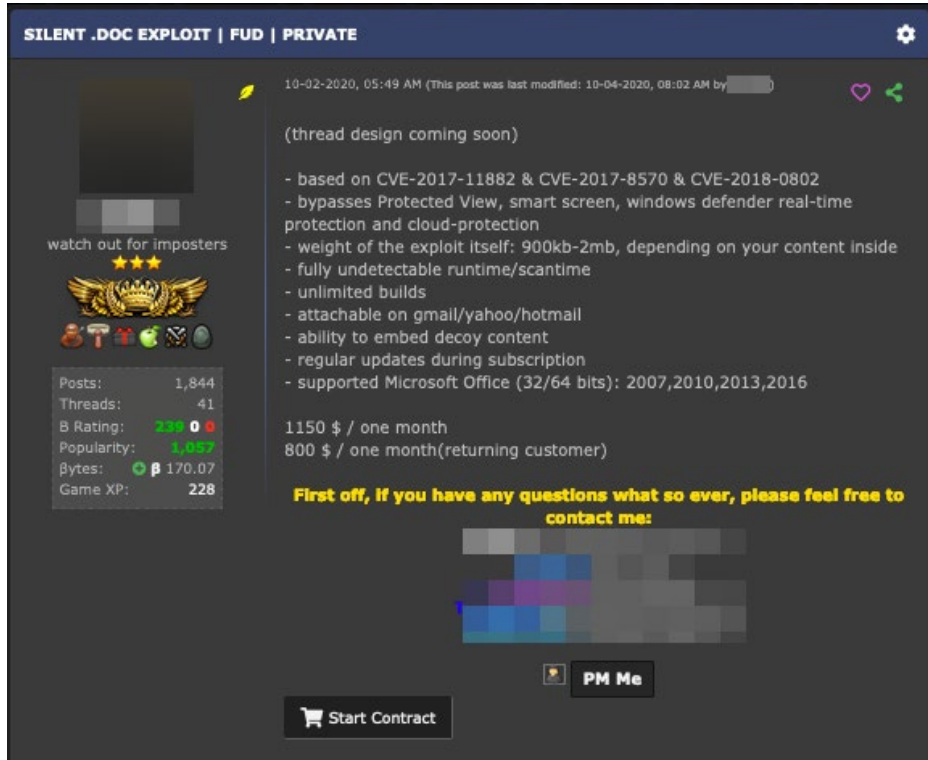


Figure 23. An English-language forum user advertising an exploit subscription service

The Future of the Exploit Market

One of the trends that could shape the future of the exploit market is the rise of the access-as-a-service model, where subscribers can access corporate networks via RDP. This offers customers advantages including ease of use and transparency, and offers vendors the chance to demand higher prices than for N-day exploits. Furthermore, access-as-a-service vendors do not get the level of scrutiny from potential buyers that exploit sellers usually receive.

It is easier to verify with just screenshots that a seller has access to the company being advertised. Prices usually start at over US\$1,000. For example, one seller offered access, using an RCE exploit, to a bank in France for US\$1,200 and a bank in Poland for US\$1,500. Vendors on RaidForums and Exploit offer a range of access-as-a-service offerings.

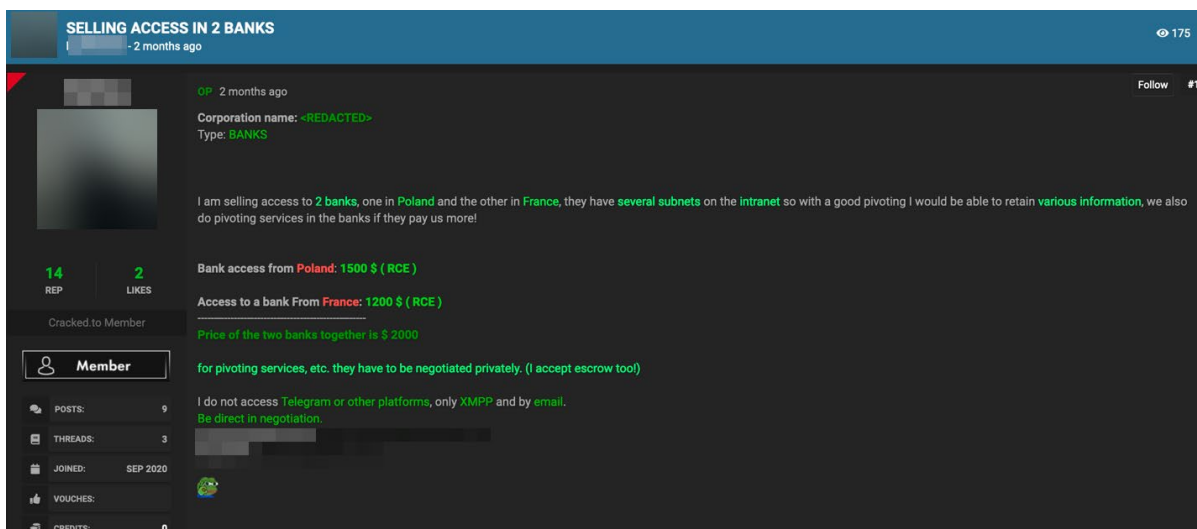


Figure 24. A forum post advertising access, using an RCE exploit, to two banks in Europe

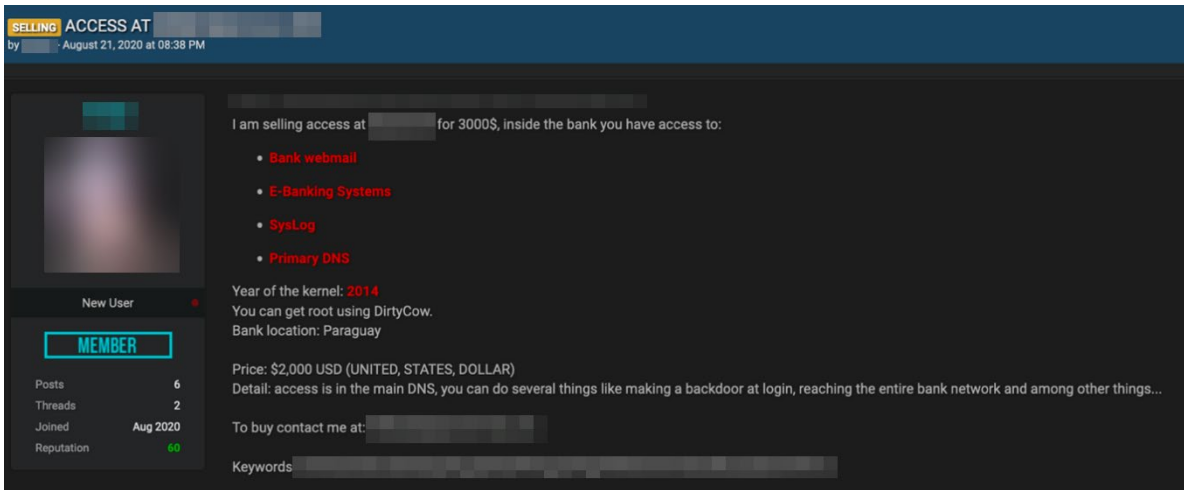


Figure 25. A forum post advertising access, using a Dirty COW exploit, to a bank

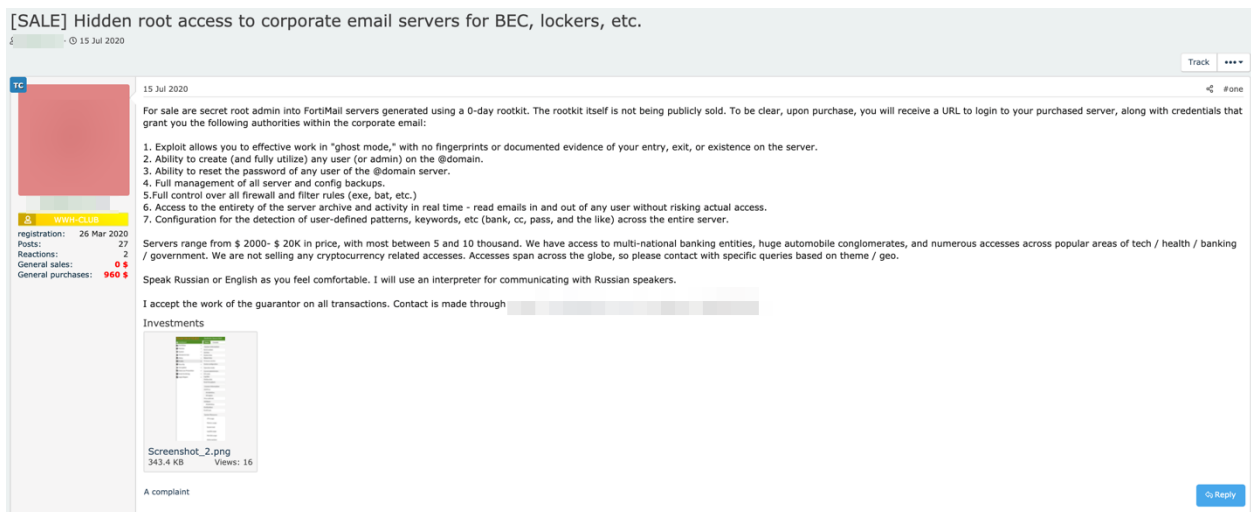


Figure 26. A forum post advertising access, using a zero-day rootkit, to email servers

We observed two types of access-as-a-service sellers: the less experienced ones and the more professional ones. The less experienced sellers typically do not dedicate all their time to access-as-a-service and mostly get lucky with finding exploits that work. The more professional sellers, on the other hand, have a wide variety of businesses available for sale and have portfolios containing mostly access-as-a-service offerings.

Conclusion

Applying all available vulnerability patches can be a nearly impossible task for any organization.¹⁴ It is simply unrealistic for organizations to have their systems be completely invulnerable. While several patch prioritization approaches exist for vulnerability management, organizations should also factor the exploits that cybercriminals actually wish to use — and can purchase — into the equation, rather than simply patching vulnerabilities based on severity, for example.

Virtual patching is one way for organizations to buy additional time needed for security teams to implement the necessary updates, making it a crucial aspect of patch management. Since vendors and manufacturers need time to come up with and deploy the necessary patches and upgrades upon the disclosure of a vulnerability, these temporary fixes give them time for permanent solutions, as well as help avoid unnecessary downtime for organizations to implement patches at their own pace. This is especially important when it comes to zero-day vulnerabilities since virtual patches protect systems and networks by serving as an additional security layer from both known and unknown exploits.

During our research, we saw the price of an exploit continually drop over time until it eventually fell to zero. This made the exploit accessible to more cybercriminals as months passed. Paradoxically, the longer the time that has passed since the release of a patch for a vulnerability, the greater the attack surface, since the pricing allows more malicious actors to incorporate the exploit for the vulnerability into their cybercriminal business models.

A key takeaway from our research is that the longevity of a valuable exploit is longer than most might expect. This is vital information for anyone who manages their organization's patch management program, since addressing yesterday's popular vulnerability can often be more important than addressing today's critical one.

References

- 1 Trend Micro. (Oct. 2, 2019). *Trend Micro*. "Security 101: Zero-Day Vulnerabilities and Exploits." Accessed on June 14, 2021, at <https://www.trendmicro.com/vinfo/ph/security/news/vulnerabilities-and-exploits/security-101-zero-day-vulnerabilities-and-exploits>.
- 2 Arjun Baltazar, Earle Maui Earnshaw, Augusto Il Remillano, and Jakub Urbanec. (March 25, 2020). *Trend Micro*. "Mirai Updates: New Variant Mukashi Targets NAS Devices, New Vulnerability Exploited in GPON Routers, UPX-Packed Fbot." Accessed on June 14, 2021, at <https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/mirai-updates-new-variant-mukashi-targets-nas-devices-new-vulnerability-exploited-in-gpon-routers-upx-packed-fbot>.
- 3 Krebs on Security. (Feb. 24, 2020). *Krebs on Security*. "Zyxel Fixes 0day in Network Storage Devices." Accessed on June 14, 2021, at <https://krebsonsecurity.com/2020/02/zyxel-fixes-0day-in-network-storage-devices/>.
- 4 Trend Micro. (April 7, 2021). *Trend Micro*. "The Nightmares of Patch Management: The Status Quo and Beyond." Accessed on June 14, 2021, at <https://www.trendmicro.com/vinfo/se/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond>.
- 5 Edgescan. (2021). *Edgescan*. "2021 Vulnerability Statistics Report." Accessed on June 14, 2021, at <https://info.edgescan.com/hubfs/Edgescan2021StatsReport.pdf?hsCtaTracking=9601b027-23d3-443f-b438-fcb671cfd06%7Cb222011c-0b6d-440b-aed8-64d37dec66e2>.
- 6 Amer Owaida. (Feb. 15, 2021). *WeLiveSecurity*. "Record-high number of vulnerabilities reported in 2020." Last accessed on June 14, 2021, at <https://www.welivesecurity.com/2021/02/15/record-breaking-number-vulnerabilities-reported-2020/>.
- 7 cve.mitre.org. (Jan. 26, 2021). *cve.mitre.org*. "CVE Program Report for Q4 Calendar Year 2020." Accessed on June 14, 2021, at https://cve.mitre.org/blog/January262021_CVE_Program_Report_for_Q4_Calendar_Year_2020.html.
- 8 Trend Micro. (Feb. 23, 2021). *Trend Micro*. "A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report." Accessed on June 14, 2021, at <https://documents.trendmicro.com/assets/rpt/rpt-a-constant-state-of-flux.pdf>.
- 9 Hassan El Hadary. (n.d.). *SANS Institute*. "SEC552: Bug Bounties and Responsible Disclosure." Accessed on June 25, 2021, at <https://www.sans.org/cyber-security-courses/bug-bounties-and-responsible-disclosure/>.
- 10 Trend Micro. (Feb. 23, 2021). *Trend Micro*. "A Constant State of Flux: Trend Micro 2020 Annual Cybersecurity Report." Accessed on June 14, 2021, at <https://documents.trendmicro.com/assets/rpt/rpt-a-constant-state-of-flux.pdf>.
- 11 Bradley Barth. (Nov. 1, 2018). *SC Magazine*. "'Outlaw' threat actor uses Shellbot variant to form new botnet." Accessed on June 14, 2021, at <https://www.scmagazine.com/home/security-news/outlaw-threat-actor-uses-shellbot-variant-to-form-new-botnet/>.
- 12 Tara Seals. (April 8, 2019). *Threatpost*. "SAS 2019: Exodus Spyware Found Targeting Apple iOS Users." Accessed on June 14, 2021, at <https://threatpost.com/exodus-spyware-apple-ios/143544/>.
- 13 Jason Gu, Veo Zhang, and Seven Shen. (Sept. 25, 2017). *Trend Micro*. "ZNIU: First Android Malware to Exploit Dirty COW." Accessed on June 14, 2021, at https://www.trendmicro.com/en_us/research/17/i/zniu-first-android-malware-exploit-dirty-cow-vulnerability.html.
- 14 Trend Micro. (April 7, 2021). *Trend Micro*. "The Nightmares of Patch Management: The Status Quo and Beyond." Accessed on June 14, 2021, at <https://www.trendmicro.com/vinfo/se/security/news/vulnerabilities-and-exploits/the-nightmares-of-patch-management-the-status-quo-and-beyond>.



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

