LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY


# TrueFighter and RDP Access

**10/08/2020**

***Report #: 202010081030***

# Agenda

- What is RDP?
- What are the Risks of RDP?
- Direct and Indirect Exploitation
- Exploit[.]In
- Threat Actor TrueFighter
- TrueFighter's August 2020 Activity
- Example: U.S. Municipal Government Center
- Mitigations
- Other Factors that Make Healthcare and Public Health (HPH) Organizations Attractive Targets

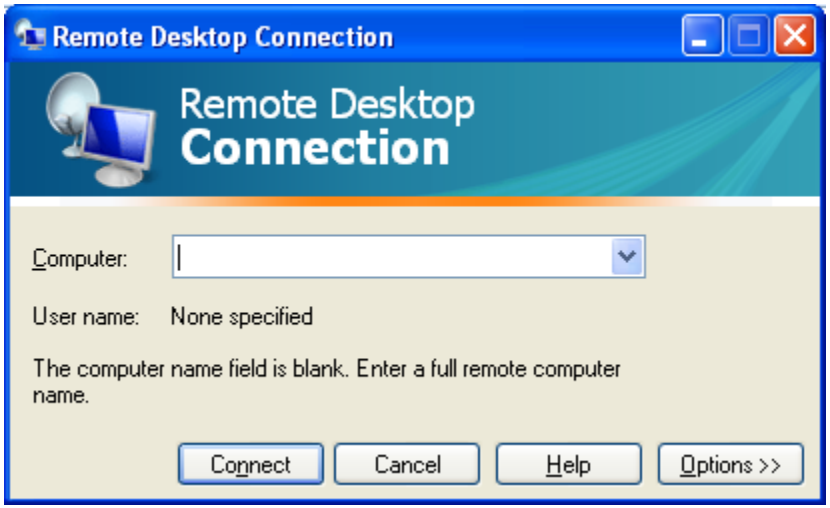
Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

# What is RDP?

- RDP access allows individuals to remotely connect with specific devices and networks
  - RDP access provides a user with a connection to a specific desktop – and all files, applications, and anything else on that desktop
  - Cloud computing provides access to files from any device
- Originally for Windows machines, it can now also be used with Apple devices
- Connects desktop computers to enterprise networks while traveling, working from home, or for IT access
- Used pre-COVID but more useful than ever:
  - Research by Shodan revealed that between January 1st and March 29th, 2020, the number of RDP endpoints increased by 40%




*Source: NetFort*

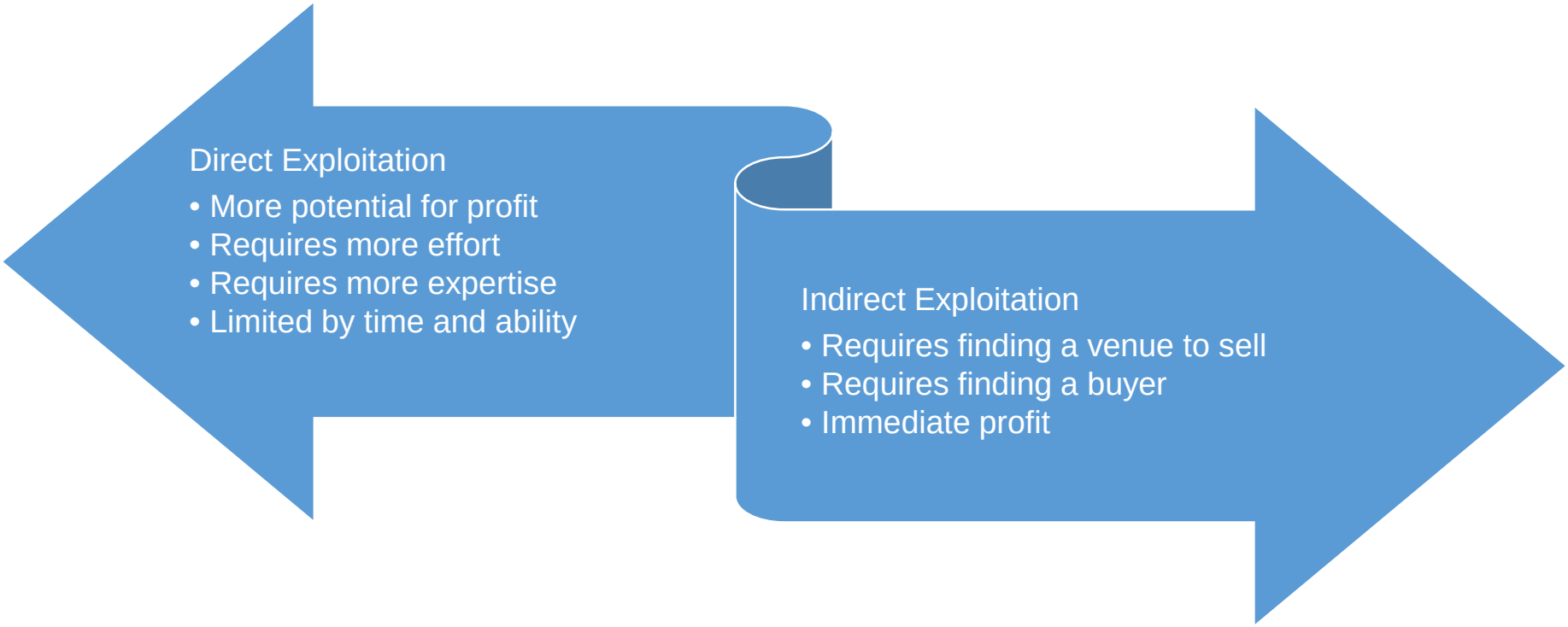
# What Are The Risks of RDP?

- Overgenerous RDP permissions can put organizations at risk
  - Organizations can disable the remote services from the Internet and restrict to internal IP address ranges only, or to only specific Internet-based addresses
- Illicit RDP access can be very valuable to threat actors targeting an organization
- Once a threat actor has RDP access, the actor has full control over the connected device and its permissions
- This access can be used to deploy malware, ransomware, or steal data from compromised devices
- Known exploits allow threat actors to fully automate the entire attack chain, including “typing” commands or passing commands to the shell
- This automation allows threat actor to attempt exploits in bulk
- Threat actors can use tools like Shodan to find vulnerable endpoints
  - Shodan is a search engine for Internet-connected devices
  - Example: A threat actor can use Shodan to find all exposed port:3389


*Source: Shodan.io*

- HealthITSecurity reported that “researchers used Shodan[.]io and found 4.3 million exposed RDP connections, with 30 percent based in the US.”
  - Exposed connections are discoverable on Shodan, but are not necessarily vulnerable to any active exploits

Once acquired, RDP access can be exploited by the threat actor directly, or advertised and sold on many dark web cybercriminal sites, including Russian-language site Exploit[.]in.



# Exploit[.]in

- High profile Russian-language cybercriminal forum on the surface web
- Operated continuously since 2005
- Experienced team of administrators
- Commonwealth of Independent States-affiliated
- Prioritizes Russian speakers, but has some content in English
- Approximately 47k members, and over one million posts as of November 2019


*Source: Digital Shadows*

# Threat Actor: TrueFighter

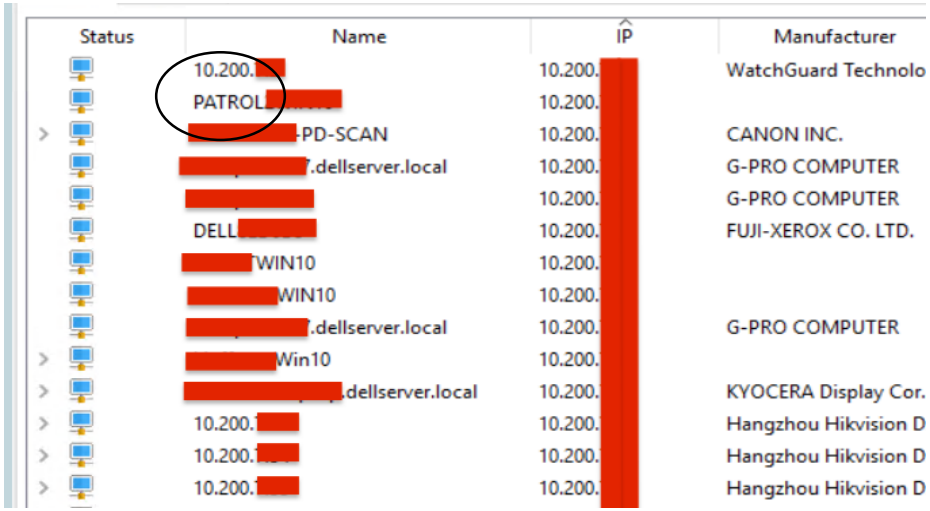
- Active on Exploit since 2014, active on other communities and forums as well
- Unknown whether single actor or group, but likely to be single actor
- Acquires and sells RDP access
- Prolific, with diverse group of targets
- Offered to upgrade RDP access to domain administrator-level access, for a fee
- Typical post does not reveal the name or identify details of the victim organization
  - o May include details like yearly revenue or number of employees
- Other forum users vouch for the quality of the advertised RDPs and endorse TrueFighter's services
- Associated actor LinuxW – aka Nikolay, aka Antony Moricone – sometimes sells the same network access credentials

*Source: BrandMatters*

| Title of Post | Description of Access | Resolution | Price (USD) |
|---|---|---|---|
| U.S. center for treatment of mental diseases and drug addiction | Admin access | Retracted after criticism from other forum users | $999 |
| U.S. government center | RDP, domain admin privileges | None | $4,000 |
| U.S. steelmaker | Admin privileges | None | $1,500 |
| U.S. family healthcare center | RDP, domain admin privileges | None | $3,000 |
| U.S. water district | Domain admin | None | $3,500 |

# Network Access to a U.S. Government Center

- Actor provided the screenshot below as proof of alleged access to a specific U.S. town – identifying details have been redacted
- Example of actor's general reliability
- Researchers verified the alleged name of the town
- Researchers identified a host named "PATROL…"
    - Potentially belonging to local law enforcement



| Status | Name | IP | Manufacturer |
|---|---|---|---|
| | 10.200.[redacted] | 10.200.[redacted] | WatchGuard Technolo |
| | PATROL[redacted] | 10.200.[redacted] | |
| | [redacted]-PD-SCAN | 10.200.[redacted] | CANON INC. |
| | [redacted].dellserver.local | 10.200.[redacted] | G-PRO COMPUTER |
| | [redacted] | 10.200.[redacted] | G-PRO COMPUTER |
| | DELL[redacted] | 10.200.[redacted] | FUJI-XEROX CO. LTD. |
| | [redacted]WIN10 | 10.200.[redacted] | |
| | [redacted]WIN10 | 10.200.[redacted] | |
| | [redacted].dellserver.local | 10.200.[redacted] | G-PRO COMPUTER |
| | [redacted]Win10 | 10.200.[redacted] | |
| | [redacted].dellserver.local | 10.200.[redacted] | KYOCERA Display Cor. |
| | 10.200.[redacted] | 10.200.[redacted] | Hangzhou Hikvision D |
| | 10.200.[redacted] | 10.200.[redacted] | Hangzhou Hikvision D |
| | 10.200.[redacted] | 10.200.[redacted] | Hangzhou Hikvision D |

**Selling access to US government center!**

I am selling access to a U.S. government center!

Population of the city: 10,000 people

Access type: RDP, domain admin privileges.

- Supervisory Board.
- Tax information.
- Municipal government.
- Public services.
- Public security.
- Resolutions.

And so on.

The number of hosts: 100.

Price: US $4,000.

Use PM!

If you are my regular customer, we can negotiate the price within reason. For the rest, the price is US $4,000.

---

UPD. Also, there's a police department on the network.

---

Aug. 24, 2020:

---

The offer is on. The price is US $3,000.

---

# Mitigations

- Because users often re-use their RDP remote login password for other services or applications, following password best practices can protect organizations against credential stuffing or brute-forcing attacks
- Password best practices include:
  - Enabling multi-factor authentication
  - Encouraging users to choose strong, unique passwords for work accounts
  - Enabling single sign-on
- Researchers also suggest restricting access to RDP connections to trusted sources and auditing connectivity logs for unknown connections
  - Defaults are TCP Port 3389 and UDP Port 3389
  - If your organization is tunneling RDP connections through a VPN, this will also protect your organization against unknown connections
- Limiting access to certain times of day
- Having access expire after a certain amount of time


*Source: SecurityMagazine*

- Another effective mitigation strategy is patching known vulnerabilities that exploit RDP access, including but not limited to:
  - **BlueKeep Vulnerability (CVE-2019-0708):** Threatens unprotected RDP servers on older Windows operating systems; allows an unauthenticated attacker to connect to the target system and execute arbitrary code on the target system
  - **CVE-2019-0863:** Runs code through the Remote Desktop functions to allow downloads, deletions, and the potential creation of new admin accounts that can lead to further attacks in the future
  - **CVE-2019-0932:** Gives malicious users access to the Skype application through Android phones, which may allow them to listen and/or record calls without the user knowing

# Other Factors Making HPH Organizations Attractive Targets

- **Vulnerable RDP connections will continue to be targeted by cyber criminals and pose an increased risk to the U.S. HPH sector**
- Cyber criminals will likely continue to target exposed RDP connections
  - Easy-to-identify exposed RDP connections using open-source tools like Shodan
  - Relatively low-risk, high-reward outcome from identifying and selling exposed RDP access
  - For the same reason that healthcare organizations are attractive targets for ransomware and malware, actors looking to exploit vulnerable RDP connections are likely to target the HPH sector
  - Organizations publicly engaged in coronavirus response or research may also be targeted to gain access to their intellectual property and data

# Reference Materials

# References


- Nuspire, TrueFighter: Remote Desktop Protocol Accounts Compromised
  - https://www.nuspire.com/blog/truefighter-remote-desktop-protocol-accounts-compromised/
- Health IT Security, Healthcare Key Target of Hacker Selling Access to Compromised RDP
  - https://healthitsecurity.com/news/healthcare-key-target-of-hacker-selling-access-to-compromised-rdp
- CloudFlare, What is the Remote Desktop Protocol (RDP)?
  - https://www.cloudflare.com/learning/access-management/what-is-the-remote-desktop-protocol/
- ZDNet, RDP and VPN use skyrocketed since coronavirus onset
  - https://www.zdnet.com/article/rdp-and-vpn-use-skyrocketed-since-coronavirus-onset/
- Digital Shadows, Forums Are Forever – Part 1: Cybercrime Never Dies
  - https://www.digitalshadows.com/blog-and-research/forums-are-forever-part-1-cybercrime-never-dies/
- CVE-2019-0708 | Remote Desktop Services Remote Code Execution Vulnerability
  - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
- NETOP, Avoid RDP Exploits with a Secure Remote Desktop
  - https://blog.netop.com/avoid-rdp-vulnerabilities-with-a-secure-remote-desktop
- SENT, Learning How To Use Shodan With RDP
  - https://www.sentandsecure.com/learning-how-to-use-shodan-with-rdp/

# Questions

## Upcoming Briefs

- Using Honeypots for Network Intrusion Detection (10/15)
- Qbot Malware (10/22)

### *Product Evaluations*

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.


HC3 Customer Feedback

### *Requests for Information*

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

### *Disclaimer*

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

*HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector*

## Products

### Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

### White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

### Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Visit us at: www.HHS.Gov/HC3

# Contact


www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV