



**State of Alaska Cyber Security &  
Critical Infrastructure  
Cyber Advisory**

**August 29, 2011**

*The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**ADVISORY NUMBER:**

SA2011-050

**DATE ISSUED:**

August 29, 2011

**SUBJECT:**

Remote Desktop Protocol Worm "Morto"

**OVERVIEW:**

There are reports of a new worm circulating that takes advantage of open port 3389/TCP to compromise systems. No user interaction is required for the host to become compromised. The worm has the capability to infect and subsequently control the impacted hosts. Anti-virus vendors are developing signatures to detect the worm.

**SYSTEMS AFFECTED:**

All versions of Windows Operating Systems

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High**

**DESCRIPTION:**

On August 27, 2011, the MS-ISAC Security Operations Center noticed an increase in Microsoft's Terminal Services traffic over port 3389/TCP across many MS-ISAC monitored networks. MS Terminal Services, also known as Remote Desktop Protocol

(RDP), allows for remote support and management of all versions of Microsoft Windows. The identified increase in traffic has primarily been the result of aggressive scanning of port 3389/TCP and login brute force attempts.

This activity was subsequently identified by anti-virus vendors as being related to a new worm known as Morto. Anti-virus vendors are developing signatures to detect the worm.

The Morto worm is able to spread by scanning for systems listening for RDP on port 3389/TCP. When Morto finds a system running RDP, it will attempt to log in with several common user names including Administrator, user, and admin. The worm will also try using a series of common passwords in order to log into the system. If the worm is successful in logging into the host, it will then use file sharing capabilities built into RDP to transfer a file to the victim in order to infect it as well. The worm will also look for and disable processes related to known anti-virus and security software. The malware will also attempt to make connections to external domains to download updates and additional components.

The Morto worm is of concern because of the potential for bandwidth consumption and more importantly, because it has the ability to be remotely controlled. This feature could allow the infected host to function like a bot or exfiltrate sensitive data.

#### **RECOMMENDATIONS:**

We recommend the following actions:

- Block port 3389 at the organization's perimeter unless there is a business need to keep the port open.
- Disable the Remote Desktop Services on all hosts which do not require the service for remote management.
- Ensure that systems are running anti-virus software and that signatures are up to date.

If Remote Desktop Services are required:

- Firewall policies should be in place that filter both ingress and egress RDP traffic between authorized hosts.
- Configure host based firewalls to allow remote management service requests from authorized hosts only.
- Utilize strong passwords that are enforced by computer and domain policies.
- Configure the RDP Server and clients to use SSL/TLS certificates for authentication.

#### **REFERENCES:**

##### **SANS ISC Diary:**

<http://isc.sans.edu/diary.html?storyid=11452&rss>

<https://isc.sans.edu/port.html?port=3389>

##### **Microsoft:**

<http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Worm%3AWin32%2FMorto.A>

<http://blogs.msdn.com/b/rds/archive/2008/07/21/configuring-terminal-servers-for-server-authentication-to-prevent-man-in-the-middle-attacks.aspx>

<http://support.microsoft.com/kb/895433>

##### **Symantec:**

[http://www.symantec.com/business/security\\_response/writeup.jsp?docid=2011-082908-4116-99](http://www.symantec.com/business/security_response/writeup.jsp?docid=2011-082908-4116-99)

**F-Secure:**

<http://www.f-secure.com/weblog/archives/00002227.html>

**Rapid7:**

<https://community.rapid7.com/community/metasploit/blog/2011/08/29/morto-another-reason-to-secure-local-user-accounts>

**The Register:**

[http://www.theregister.co.uk/2011/08/28/morto\\_worm\\_spreading/](http://www.theregister.co.uk/2011/08/28/morto_worm_spreading/)