dnssd
Internet-Draft
Intended status: Informational
Expires: November 20, 2015

D. Otis
Trend Micro

May 19, 2015

mDNS X-link review
draft-otis-dnssd-mdns-xlink-06

Abstract

Multicast DNS will not normally extend beyond the MAC Bridge. This limitation is problematic when desired services are beyond the reach of multicast mDNS. This document explores security considerations when overcoming this limitation.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on November 20, 2015.

Copyright Notice

Table of Contents

1. Introduction

On Bridged LANs, as described by [IEEE.802-1D.2004], MAC entities make their services known via multicast. Multicast forms a basis for networking and layer 3 protocol initialization where [mDNS] together with [DNS-SD] provide a higher level of structure based on multicast announcements made within a LAN environment. Unfortunately, an increased exchange of structural information does not scale well. There is an effort to push mDNS into DNS. Just exposure of [mDNS] to the Internet has proven problematic as noted by [CERTvu550620]. [DNS-SD] can further extend DDoS amplification concerns. [mDNS] may use Jumbo frames of 9000 bytes that exceeds design limits of Ethernet CRC, however it recommends an upper limit of 1,300 bytes suitable for most local networks. DNS started with in an era working within the minimum MTU established by [RFC0791] and noted by [RFC1191] of 576 bytes which accommodates 512 byte UDP DNS messages. Most Internet links are able to handle larger MTUs, as per the minimum 1280 byte MTU specified by [RFC2460] for IPv6.

[DNS-SD] discovery is initialized by querying DNS PTR queries using Unicast or Multicast DNS at five special zones reserved for this purpose:

b._dns-sd._udp.<Domain>. Domain list to Browse

db._dns-sd._udp.<Domain>. Default Domain to Browse

r._dns-sd._udp.<Domain>. Domains list to register service

dr._dns-sd._udp.<Domain>. Default Domain to register service

lb._dns-sd._udp.<Domain>. Legacy Browse using special label info

SRV [RFC2782] records are located with the form:
"_<sn>._<Proto>.<Domain>

DNS-SD differs by locating SRV and TXT RR-sets with the forms:

_<sn>._<Proto>.<SrvDOM>.<ParentDOM>.

<Instance>._<sn>._<Proto>.<SrvDOM>.<ParentDOM>.

<sub>._sub._<sn>._<Proto>.<SrvDOM>.<ParentDOM>.

Instance names are not host names and may use Unicode for Network Interchange [RFC5198] encoding and may include escaped periods "\." and other punctuation and spaces.

For DNS-SD, Proto="udp" for all non-TCP transports otherwise it is "tcp" .

_<sn> = IANA Registered Service Name

At each of these locations SRV and TXT Resource Record Sets offer instance and service enumerations but resulting RR-sets may be unsuitable for exposure to the Internet. The RR-sets returned in response to a wildcard placed at the instance location can approach 839 instances and 64 kBytes. In addition, a browsing operation never completes until terminated where clients are expected to report availability state changes. The DNS-SD query to response ratio makes it potentially unsuitable for access over the Internet.

A Bridge acts as an interconnect mechanism transparent to end stations on LANs. Bridges designated to forward frames is normally accomplished by participation in a Spanning Tree Algorithm. Many expect [mDNS] resource records can be safely and automatically placed into [DNS] to overcome Bridge to Bridge multicast limitations. Nevertheless, such a process must operate in conjunction with requisite controls necessary to retain network security.

A Bridge forwards frames based on prior source MAC associations with incoming frames on different LAN ports. Source MAC and LAN port associations are recommended to expire in 300 seconds. Frames containing source multicast MACs are silently discarded as invalid. Frames containing a destination MAC on the same LAN port already associated with the MAC are silently discarded. A valid incoming frame with a destination not previously associated with a different LAN port is forwarded (flooded) to all other LAN ports, otherwise when a MAC destination address is associated with a different LAN port from which the frame was received, the frame is selectively forwarded to this port. All broadcast and multicast MACs are flooded to all other LAN ports because they do not represent a valid source. Flooding operations may create a storm of replicated frames having an unknown MAC destination whenever forwarding is enabled on LAN ports connected in a loop.

In [IEEE.802-11.2012] wireless networks, multicast frames are transmitted at a low data rate supported by all receivers. Multicast on wireless networks may thereby lower overall network throughput. Some network administrators block some multicast traffic or convert it to a series of link-layer unicast frames.

Wireless links may be orders of magnitude less reliable than their wired counterparts. To improve transmission reliability, [IEEE.802-11.2012] requires positive acknowledgement of unicast frames. It does not, however, support positive acknowledgement of

multicast frames. As a result, it is common to observe much higher loss of multicast frames on wireless compared against wired network technologies.

2. IANA Considerations

This document requires no IANA consideration.

3. Security Considerations

Scalable DNS-SD (SSD) proposes to automatically gather autonomously named [mDNS] resource records by observing announcement traffic to then make routable resources visible and accessible from other networks via unicast [DNS] structured per [DNS-SD]. When doing so, address translation using Unique Local Addresses, ULAs [RFC4193] can offer a significant level of protection since typical link-local addresses are not usable from other networks but either ULA or [RFC1918] addresses typically indicate site local. Section 3.2 of [RFC4193] are locally defined and handled as Global addresses although not intended to be routed beyond the site or beyond those having explicit routing agreements.

Section 4.1 of [RFC4193] indicates the default behavior of exterior routing protocol sessions between administrative routing regions must be to ignore receipt of and not advertise prefixes in the FC00::/7 block. A network operator may specifically configure prefixes longer than FC00::/7 for inter-site communication. Specifically, these prefixes are not designed to aggregate. Routers by default do not block ULA prefixes which makes it important to confirm how ULA traffic is handled by the access provider.

ULA or [RFC1918] addresses are not normally routed over the Internet where their use provides a degree of isolation. For either home or enterprise networks, ULAs as an overlay network avoids network address translations and permits local routing isolated from direct Internet access. ULAs also permit local communications to remain unaffected by Internet related link failures or scope limitations imposed by use of multicast protocols.

ULAs avoid a need to renumber internal-only private nodes when changing ISPs, or when ISPs restructure their address allocations. In these situations, use of ULA offers an effective tool for protecting internal-only nodes. As such, more than just the security considerations discussed in [mDNS] and [DNS-SD] are needed. For example, [DNS-SD] states the following: "Since DNS-SD is just a specification for how to name and use records in the existing DNS, it

has no specific additional security requirements over and above those that already apply to DNS queries and DNS updates." This simply overlooks that many devices are not automatically published in DNS nor can it be assumed they are able to handle the access that DNS might permit.

[DNS-SD] recommends additional DNS records such as the associated PTR and TXT SHOULD be generated to improve network efficiency for both Unicast and Multicast DNS-SD responses. This behavior further increases risks related to query/response ratios and the likelihood security sensitive information might become exposed.

Current BTMM [RFC6281] only publishes ULAs of hosts in DNS able to authenticate when setting up an overlay network. Remaining devices, such as printers, are only accessed as shared elements offered by the authenticating hosts. DNS resources should never be considered to offer privacy even in split-horizon configurations. DNS is unable to authenticate incoming queries nor can it offer application layer protection. Since many prefixes are expected to be in use within environments served by [I-D.cheshire-dnssd-hybrid], errors related to network boundary detections becomes critical. As such, DNS SHOULD NOT publish addresses of devices unable to authenticate sessions that traverse the Internet.

[DNS-SD] should not be viewed as only a catalog structure of desired services. [I-D.cheshire-dnssd-hybrid] is to be used to bridge adjacent networks, which risks conveying resources of hosts that are unable to safely facilitate Internet access. Since [I-D.cheshire-dnssd-hybrid] only expects to disclose routable addresses while also ignoring use of ULAs, this clearly expects conveyance of globally routable addresses, GUA. Use of ULAs instead of GUAs represents a significantly safer strategy that permits limited devices to remain isolated from the Internet while still allowing packet routing between local network realms.

[I-D.cheshire-dnssd-hybrid] lacks a process able to limit resources being gathered, resolved, and propagated to those that can be administrated. As such, an [I-D.cheshire-dnssd-hybrid] scheme represents a profound change to network security. The following sections highlight potential threats posed by deploying [DNS-SD] over multiple links through the automated collection and publication of [mDNS] resources into [DNS] as proposed by [I-D.cheshire-dnssd-hybrid]. This conveyance expands namespaces into .local., .sitelocal., and [DNS] which may also cache Internet namespace.

This new routable namespace also lacks the benefit of registrar involvement and may not afford an administrator an ability to

mitigate nefarious activity, such as spoofing and phishing, without requisite controls having been first carefully established. When a device has access to different realms on multiple interfaces, it is not even clear how simple conflict resolution avoids threatening network stability while resolving names conveyed over disparate technologies.

Managing autonomously named resources becomes especially salient since visually selected names are not ensured uniquely represented nor quickly resolved due to latency uncertainties. For example, [DNS] recommends 5 second timeouts with a doubling on two subsequent retries for a total of 35 seconds. [mDNS] only requires compliance with [RFC5198] rather than IDNA2008 [RFC5895]. This less restrictive use of the name space may impair the defense of critical services from look-alike attack. [mDNS] does not ensure instances are visually unique and allows spaces and punctuation not permitted by IDNA2008.

It is imperative for SSD to include requisite filtering necessary to prevent data ex-filtration or the interception of sensitive services. Any exchanged data must first ensure locality, limit the resources gathered, resolved, and propagated to just those elements that can be effectively administrated. It is critical to ensure normal network protection is not lost for hosts that depend on link-local addressing and exclusion of routable traffic. A printer would be one such example of a host that can not be upgraded.

3.1. Multiple Link Strategies

3.1.1. Selective Forwarding based on IGMP or MLD snooping

Internet Group Management Protocol (IGMP) [RFC3376] supports multicast on IPv4 networks. Multicast Listener Discovery (MLD) [RFC3810] supports multicast management on IPv6 networks using ICMPv6 messaging in contrast to IGMP's bare IP encapsulation. This management allows routers to announce their multicast membership to neighboring routers. To optimize which LANs receive forwarded multicast frames, IGMP or MLD snooping can be used to determine the presence of listeners as a means to permit selective forwarding of multicast frames as well.

3.1.2. IPv4 Link-Local

[RFC3927] provides an overview of IPv4 address complexities related to dealing with multiple segments and interfaces. IPv6 introduces new paradigms in respect to interface address assignments which offer scoping as explained in [RFC4291].

3.1.3. VLAN

Use of VLAN such as [RFC5517] can selectively extend multicast forwarding beyond Bridge limitations. While not a general solution, use of VLAN can both isolate and unite specific networks.

3.1.4. DHCP

IP address assignment and host registration might use a single or forwarded DHCP [RFC2131] or [RFC3315] server for IPv4 and IPv6 respectively that responds to interconnected networks as a means to register hosts and addresses. DHCP does not ensure against name or address conflict nor is it intended to configure routers.

3.1.5. Automated placement of mDNS resources into DNS

IP addresses made visible by [DNSSEC] or [DNS] that conform with [DNS-SD] might be used, but the automated population of information into [DNS] should be limited to administrative systems.

Automated conversion of [mDNS] into unicast [DNS] can be problematic from a security standpoint as can the widespread propagation of multicast frames. [mDNS] only requires compliance with [RFC5198] rather than IDNA2008 [RFC5895]. This means [mDNS] does not ensure instances are visually unique and may contain spaces and punctuation not permitted by IDNA2008. As such, this might allow users into becoming misled about the scope of a name.

Replacing ASCII punctuation and spaces in the label with the '_' character, except when located as the leftmost character, may reduce some handling issues related to end of string parsing, since labels in [DNS] normally do not contain spaces or punctuation. Nevertheless, [DNS] is able to handle such labels within sub-domains of registered domains.

Services outside the ".local." domain may have applications obtaining domain search lists provided by DHCP ([RFC2131] and [RFC3315] for IPv4 and IPv6 respectively or RA DNSSL [RFC6106] also for IPv6. Internet domains need to be published in [DNS] as A-Labels [RFC3492] because IDNA2008 compliance depends on A-label enforcement by registrars. Therefore A-Labels and not U-Labels must be published in DNS for Internet domains at this time.

The SRV scheme used by [mDNS] has also been widely adopted in the Windows OS since it offered a functional replacement for Windows Internet Name Service (WINS) as their initial attempt which lacked sufficient name hierarchy. Such common use may represent security considerations whenever these records can be automatically published.

It is unknown whether sufficient filtering of [mDNS] to expose just those services likely needed will sufficiently protect wireless networks. The extent of using IGMP or MLD for selective forwarding to mitigate otherwise spurious traffic is unknown.

ULA or [RFC1918] addresses allow safer automatic publication in DNS since these addresses are unlikely to be routed beyond the site. These addresses also provide a simple scheme to ascertain which addresses should be blocked at a network boundary. The use of other addresses MUST require specific administrative confirmations. It should be noted in the Addendum example, the Brother printer published a globally routable address.

3.2. Scope of Discovery

As [mDNS] is currently restricted to a single link, the scope of the advertisement is limited, by design, to the shared link between client and the device offering a service. In a multi-link scenario, the owner of the advertised service may not have a clear indication of the scope of its advertisement.

If the advertisement propagates to a larger set of links than expected, this may result in unauthorized clients (from the perspective of the owner) connecting to the advertised service. It also discloses information (about the host and service) to a larger set of potential attackers.

If the scope of the discovery is not properly setup or constrained, then information leaks will happen beyond the appropriate network which may also expose the network to various forms of attack as well.

3.3. Multiple Namespaces

There is a possibility of conflicts between local, multi-realm, and global [DNS] namespaces. Without adequate feedback, a client may not know whether the target service is the correct one, which can therefore enable potential attacks.

A Host unable to recognize when it is in conflict with itself over multiple realms also represents a potential network stability threat.

3.4. Authorization

[DNSSEC] can assert the validity but not the veracity of records in a zone file. The trust model of the global [DNS] relies on the fact that human administrators either a) manually enter resource records into a zone file, or b) configure the [DNS] server to authenticate a trusted device (e.g., a DHCP server) that can automatically maintain

such records.

An imposter may register on the local link and appear as a legitimate service. Such "rogue" services may then be automatically registered in wide area [DNS-SD].

3.5. Authentication

Up to now, the "plug-and-play" nature of [mDNS] devices have relied only on physical connectivity to the local network. If a device is visible via [mDNS], it had been assumed to be trusted. When multiple networks are involved, verifying a host is local using [mDNS] is no longer possible so other verification schemes must be used.

3.6. Privacy Considerations

Mobile devices such as smart phones that can expose the location of their owners by registering services in arbitrary zones pose a risk to privacy. Such devices must not register their services in arbitrary zones without the approval of their operators. However, it should be possible to configure one or more "safe" zones, e.g., based on subnet prefix, in which mobile devices may automatically register their services.

As noted in [CERTvu550620] private security information is leaked in many cases. This includes hostnames and MACs, networking details, service related details such as those for Printers and NAS devices. Many consumer printers can not authenticated users or block addresses when connected with IPv6. Once this information is leaked, malefactors are given unlimited access.

4. Acknowledgements

The authors wish to acknowledge valuable contributions from the following: Dave Rand, Michael Tuexen, Hosnieh Rafiee

5. References

5.1. Normative References

[DNS] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[DNS-SD] Cheshire, S. and M. Krochmal, "DNS-Based Service

Discovery", RFC 6763, February 2013.

[DNSSEC] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

[RFC2782] Gulbrandsen, A., Vixie, P., and L. Esibov, "A DNS RR for specifying the location of services (DNS SRV)", RFC 2782, February 2000.

[RFC3492] Costello, A., "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, March 2003.

[RFC3587] Hinden, R., Deering, S., and E. Nordmark, "IPv6 Global Unicast Address Format", RFC 3587, August 2003.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC5198] Klensin, J. and M. Padlipsky, "Unicode Format for Network Interchange", RFC 5198, March 2008.

[RFC5895] Resnick, P. and P. Hoffman, "Mapping Characters for Internationalized Domain Names in Applications (IDNA) 2008", RFC 5895, September 2010.

[RFC6106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 6106, November 2010.

[mDNS] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762,

February 2013.

5.2. References - Informative

[CERTvu550620]
Seaman, C., "CERT Vulnerability Note VU#550620", March 2015, <https://www.kb.cert.org/vuls/id/550620>.

[I-D.cheshire-dnssd-hybrid]
Cheshire, S., "Hybrid Unicast/Multicast DNS-Based Service Discovery", draft-cheshire-dnssd-hybrid-01 (work in progress), January 2014.

[I-D.ietf-dnssd-push]
Pusateri, T. and S. Cheshire, "DNS Push Notifications", draft-ietf-dnssd-push-00 (work in progress), March 2015.

[I-D.ietf-dnssd-requirements]
Lynn, K., Cheshire, S., Blanchet, M., and D. Migault, "Requirements for Scalable DNS-SD/mDNS Extensions", draft-ietf-dnssd-requirements-06 (work in progress), March 2015.

[IEEE.802-11.2012]
"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", IEEE Standard 802.11, February 2012, <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>.

[IEEE.802-1D.2004]
Institute of Electrical and Electronics Engineers, "Information technology - Telecommunications and information exchange between systems - Local area networks - Media access control (MAC) bridges", IEEE Standard 802.1D, February 2004, <http://standards.ieee.org/getieee802/download/802.1D-2004.pdf>.

[IEEE.802-3.2012]
"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications"", IEEE Standard 802.3, August 2012, <http://standards.ieee.org/getieee802/download/

802.3-2012_section1.pdf>.

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, September 1981.

[RFC1112] Deering, S., "Host extensions for IP multi-casting", STD 5, RFC 1112, August 1989.

[RFC1191] Mogul, J. and S. Deering, "Path MTU discovery", RFC 1191, November 1990.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3376] Cain, B., Deering, S., Kouvelas, I., Fenner, B., and A. Thyagarajan, "Internet Group Management Protocol, Version 3", RFC 3376, October 2002.

[RFC3810] Vida, R. and L. Costa, "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, June 2004.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, May 2005.

[RFC4043] Pinkas, D. and T. Gindin, "Internet X.509 Public Key Infrastructure Permanent Identifier", RFC 4043, May 2005.

[RFC4510] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, June 2006.

[RFC4541] Christensen, M., Kimball, K., and F. Solensky, "Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches", RFC 4541, May 2006.

[RFC5517] HomChaudhuri, S. and M. Foschiano, "Cisco Systems' Private VLANs: Scalable Security in a Multi-Client Environment", RFC 5517, February 2010.

[RFC6281] Cheshire, S., Zhu, Z., Wakikawa, R., and L. Zhang, "Understanding Apple's Back to My Mac (BTMM) Service", RFC 6281, June 2011.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, April 2014.

Appendix A. mDNS Example of Device Resolution Information

```
dns-sd -L "Brother MFC-9560CDW" _printer._tcp local
  Lookup Brother MFC-9560CDW._printer._tcp.local

16:00:26.965  Brother\032MFC-9560CDW._printer._tcp.local.
 can be reached at BRN30066C239958.local.:515
(interface 4) Flags: 2 txtvers=1 qtotal=1
pdl=application/vnd.hp-PCL,application/vnd.brother-hbp
rp=duerqxesz5090 ty=Brother\ MFC-9560CDW product=\(Brother\ MFC-9560CDW\)
adminurl=http://BRN30066C239958.local./
priority=75 usb_MFG=Brother usb_MDL=MFC-9560CDW
Color=T Copies=T Duplex=F PaperCustom=T Binary=T Transparent=T TBCP=F

Timestamp     A/R Flags if Hostname         Address                     TTL
16:14:34.855  Add     3  4 BRN30066C239958.local.
                           192.168.99.99                               245
16:14:34.856  Add     2  4 BRN30066C239958.local.
                           2699:9999:7300:1510:3205:5CFF:FE23:9958%<0> 245

dns-sd -L "Canon MX920 series" _printer._tcp local.
Lookup Canon MX920 series._printer._tcp.local.

16:47:09.676  Canon\032MX920\032series._printer._tcp.local.
 can be reached at 9299990000.local.:515 (interface 4) Flags: 2
 txtvers=1 rp=auto note= qtotal=1 priority=60 ty=Canon\ MX920
 \ series product=\(Canon\ MX920\ series\)
 pdl=application/octet-stream adminurl=http://929999000000.local.
 usb_MFG=Canon usb_MDL=MX920\ series
 usb_CMD= UUID=00000000-0000-1000-8000-F4813999999
 Color=T Duplex=T Scan=T Fax=F mac=F4:81:39:99:99:99

dns-sd -G v4v6 "9299999000000.local."
Timestamp     A/R Flags if Hostname         Address                     TTL
17:07:12.460  Add     3  4 929999000000.local.
                           FE80:0000:0000:0000:F681:39FF:FE92:9999%en0  65
17:07:12.461  Add     2  4 929999000000.local.
                           192.168.99.108                               65
```

Appendix B. Uncontrolled Access Example

The risk is that adequate IPv6 filtering is simply not available on either current printers, scanners, cameras and other devices that were never intended to be used directly on the Internet.

For example, in the case of a printer:

```
ftp [DNS entry]

Trying 2699:9999:7300:1510:3205:5cff:fe23:9958...
Connected to [DNS entry]
220 FTP print service:V-1.13/Use the network password for the ID if
updating.
Name (BRN30066C239958.local.:dlr): ftp
230 User ftp logged in.
ftp> ls
229 Entering Extended Passive Mode (|||62468|)
150 Transfer Start
total 1
-r--r--r--   1 root     printer   4096 Sep 28  2001 CFG-PAGE.TXT
----------   1 root     printer      0 Sep 28  2001 Toner-Low-------
226 Data Transfer OK.
ftp>
```

From here, I can print a file with no further authentication. But the printer also now appears on the Internet with TCP ports 21,23,25,80,515,631 and 9100 active. I can scan a document that was left in the flatbed. I can send a fax. Or I can print many copies of black pages if I want to do a physical DOS. And, thanks to the globally routable address present, I can reach this from anywhere in the world.

Author's Address

Douglas Otis
Trend Micro
10101 N. De Anza Blvd
Cupertino, CA 95014
USA

Phone: +1.408.257-1500
Email: doug_otis@trendmicro.com