THE CITY OF
CHARLOTTE
MICHIGAN

Manager's Report
February 16th Council Meeting

Ice Rink
The ice rink is frozen and open for skaters. A big kudos to the Department of Public Works and Fire Department for their hard work to get the rink ready for use. Enjoy some outdoor winter fun!

Fire Department Report
The year-to-date run totals and historical run totals for the fire department are included for Council's review.

Building Permit Services
Discussions with the county's building official have begun regarding transition of building permitting services upon the departure of the Fire Chief/Building Official. This process will include considerations for the transition of building permit data via BS&A software, process for managing open permits, process for managing new submittals and coordination of service with the Community Development Director, among others. Given that the County currently issues our trade permits, we anticipate this will be accomplished with minimal-no disruption to services. The process will include the City formally sending notice to the state that we would like the County to administer our construction code and we will have to rescind our ordinance.

IT Update
A recent NY Times article reported on a recent attack on a water plant in Florida. The persons infiltrated the system and attempted to change levels of chemical treatments such that could have posed harm to public health. Fortunately for the citizens of that community, the attack was caught before anyone was harmed. These types of incidents serve as important reminders to the critical role IT plays in the safe and effective operations of municipal government. I am proud to report the City of Charlotte has robust protection of its digital infrastructure, including safeguards that would prevent against this style of attack on our systems. I have included the detailed response from our IT consultant about this matter for Council's review.

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA21-042A

February 11, 2021

Compromise of U.S. Water Treatment Facility

SUMMARY

On February 5, 2021, unidentified cyber actors obtained unauthorized access to the supervisory control and data acquisition (SCADA) system at a U.S. drinking water treatment plant. The unidentified actors used the SCADA system's software to increase the amount of sodium hydroxide, also known as lye, a caustic chemical, as part of the water treatment process. Water treatment plant personnel immediately noticed the change in dosing amounts and corrected the issue before the SCADA system's software detected the manipulation and alarmed due to the unauthorized change. As a result, the water treatment process remained unaffected and continued to operate as normal. The cyber actors likely accessed the system by exploiting cybersecurity weaknesses, including poor password security, and an outdated operating system. Early information indicates it is possible that a desktop sharing software, such as TeamViewer, may have been used to gain unauthorized access to the system. Onsite response to the incident included Pinellas County Sheriff Office (PCSO), U.S. Secret Service (USSS), and the Federal Bureau of Investigation (FBI).

The FBI, the Cybersecurity and Infrastructure Security Agency (CISA), the Environmental Protection Agency (EPA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) have observed cyber criminals targeting and exploiting desktop sharing software and computer networks running operating systems with end of life status to gain unauthorized access to systems. Desktop sharing software, which has multiple legitimate uses—such as enabling telework, remote technical support, and file transfers—can also be exploited through malicious actors' use of social engineering tactics and other illicit measures. Windows 7 will become more susceptible to exploitation due to lack of security updates and the discovery of new vulnerabilities. Microsoft and other industry professionals strongly recommend upgrading computer systems to an actively supported operating system. Continuing to use any operating system within an enterprise beyond the end of life status may provide cyber criminals access into computer systems.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by e-mail at CyWatch@fbi.gov or your local WMD Coordinator. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at Central@cisa.gov.

THREAT OVERVIEW

Desktop Sharing Software

The FBI, CISA, EPA, and MS-ISAC have observed corrupt insiders and outside cyber actors using desktop sharing software to victimize targets in a range of organizations, including those in the critical infrastructure sectors. In addition to adjusting system operations, cyber actors also use the following techniques:

- Use access granted by desktop sharing software to perform fraudulent wire transfers.
- Inject malicious code that allows the cyber actors to
    - Hide desktop sharing software windows;
    - Protect malicious files from being detected; and,
    - Control desktop sharing software startup parameters to obfuscate their activity.
- Move laterally across a network to increase the scope of activity.

TeamViewer, a desktop sharing software, is a legitimate popular tool that has been exploited by cyber actors engaged in targeted social engineering attacks, as well as large scale, indiscriminate phishing campaigns. Desktop sharing software can also be used by employees with vindictive and/or larcenous motivations against employers.

Beyond its legitimate uses, TeamViewer allows cyber actors to exercise remote control over computer systems and drop files onto victim computers, making it functionally similar to Remote Access Trojans (RATs). TeamViewer's legitimate use, however, makes anomalous activity less suspicious to end users and system administrators compared to RATs.

Windows 7 End of Life

On January 14, 2020, Microsoft ended support for the Windows 7 operating system, which includes security updates and technical support unless certain customers purchased an Extended Security Update (ESU) plan. The ESU plan is paid per-device and available for Windows 7 Professional and Enterprise versions, with an increasing price the longer a customer continues use. Microsoft will only offer the ESU plan until January 2023. Continued use of Windows 7 increases the risk of cyber actor exploitation of a computer system.

Cyber actors continue to find entry points into legacy Windows operating systems and leverage Remote Desktop Protocol (RDP) exploits. Microsoft released an emergency patch for its older operating systems, including Windows 7, after an information security researcher discovered an RDP vulnerability in May 2019. Since the end of July 2019, malicious RDP activity has increased with the development of a working commercial exploit for the vulnerability. Cyber actors often use misconfigured or improperly secured RDP access controls to conduct cyberattacks. The xDedic Marketplace, taken down by law enforcement in 2019, flourished by compromising RDP vulnerabilities around the world.

MITIGATIONS

General Recommendations

The following cyber hygiene measures may help protect against the aforementioned scheme:

- Update to the latest version of the operating system (e.g. Windows 10).
- Use multiple-factor authentication.
- Use strong passwords to protect Remote Desktop Protocol (RDP) credentials.
- Ensure anti-virus, spam filters, and firewalls are up to date, properly configured and secure.
- Audit network configurations and isolate computer systems that cannot be updated.
- Audit your network for systems using RDP, closing unused RDP ports, applying multiple-factor authentication wherever possible, and logging RDP login attempts.
- Audit logs for all remote connection protocols.
- Train users to identify and report attempts at social engineering.
- Identify and suspend access of users exhibiting unusual activity.

Water and Wastewater Systems Security Recommendations

The following physical security measures serve as additional protective measures:

Install independent cyber-physical safety systems. These are systems that physically prevent dangerous conditions from occurring if the control system is compromised by a threat actor.

- Examples of cyber-physical safety system controls include:
  - Size of the chemical pump
  - Size of the chemical reservoir
  - Gearing on valves
  - Pressure switches, etc.

The benefit of these types of controls in the water sector is that smaller systems, with limited cybersecurity capability, can assess their system from a worst-case scenario. The operators can take physical steps to limit the damage. If, for example, cyber actors gain control of a sodium hydroxide pump, they will be unable to raise the pH to dangerous levels.

TeamViewer Software Recommendations

For a more secured implementation of TeamViewer software:

- Do not use unattended access features, such as “Start TeamViewer with Windows” and “Grant easy access.”
- Configure TeamViewer service to “manual start,” so that the application and associated background services are stopped when not in use.
- Set random passwords to generate 10-character alphanumeric passwords.
- If using personal passwords, utilize complex rotating passwords of varying lengths. **Note:** TeamViewer allows users to change connection passwords for each new session. If an end user chooses this option, never save connection passwords as an option as they can be leveraged for persistence.

- When configuring access control for a host, utilize custom settings to tier the access a remote party may attempt to acquire.
- Require remote party to receive confirmation from the host to gain any access other than "view only." Doing so will ensure that, if an unauthorized party is able to connect via TeamViewer, they will only see a locked screen and will not have keyboard control.
- Utilize the 'Block and Allow' list which enables a user to control which other organizational users of TeamViewer may request access to the system. This list can also be used to block users suspected of unauthorized access.

CHARLOTTE FIRE DEPARTMENT

FIRE RUN TOTALS

	2016			2017			2018			2019			2020			2021		
	RUNS THIS MONTH		YEAR TO DATE	RUNS THIS MONTH		YEAR TO DATE	RUNS THIS MONTH		YEAR TO DATE	RUNS THIS MONTH		YEAR TO DATE	RUNS THIS MONTH		YEAR TO DATE	RUNS THIS MONTH		YEAR TO DATE
JANUARY	46	---	46	65	---	65	67	---	67	70	---	70	42	---	42	71	---	71
FEBRUARY	60	---	106	42	---	107	55	---	122	55	---	125	58	---	100		---	
MARCH	50	---	156	86	---	193	63	---	185	66	---	191	47	---	147		---	
APRIL	44	---	200	47	---	240	99	---	284	53	---	244	51	---	198		---	
MAY	50	---	250	59	---	299	67	---	351	56	---	300	54	---	252		---	
JUNE	46	---	296	52	---	351	59	---	410	73	---	373	99	---	351		---	
JULY	56	---	352	84	---	435	81	---	491	72	---	445	80	---	431		---	
AUGUST	49	---	401	57	---	492	71	---	562	58	---	503	64	---	495		---	
SEPTEMBER	54	---	455	81	---	573	53	---	615	58	---	561	74	---	569		---	
OCTOBER	47	---	502	64	---	637	48	---	663	59	---	620	64	---	633		---	
NOVEMBER	56	---	558	56	---	693	59	---	722	56	---	676	85	---	718		---	
DECEMBER	55	---	613	62	---	755	50	---	772	57	---	733	67	---	785		---	

	2021			DEVIATION FROM LAST YEAR		5 YEAR AVERAGE		DEVIATION FROM 5 YR AVERAGE		15 YEAR AVERAGE		DEVIATION FROM 15 YR AVERAGE	
	RUNS THIS MONTH		YEAR TO DATE	RUNS THIS MONTH	YEAR TO DATE	RUNS THIS MONTH	YEAR TO DATE	RUNS THIS MONTH	YEAR TO DATE	RUNS THIS MONTH	YEAR TO DATE	RUNS THIS MONTH	YEAR TO DATE
JANUARY	71	--	71	29	29	58	58	13	13	47	47	24	24
FEBRUARY		--				54	112			43	90		
MARCH		--				62	174			53	142		
APRIL		--				59	233			50	192		
MAY		--				57	290			51	244		
JUNE		--				66	356			49	293		
JULY		--				75	431			60	352		
AUGUST		--				60	491			48	401		
SEPTEMBER		--				64	555			51	451		
OCTOBER		--				56	611			49	501		
NOVEMBER		--				62	673			48	549		
DECEMBER		--				58	732			57	606		

MOST / LEAST RUNS PER MONTH 1976 THRU 2021

	MOST			LEAST		
JANUARY	**2021**	=	**71**	1976	=	7
FEBRUARY	2016	=	60	1986	=	9
MARCH	2017	=	86	1980	=	15
APRIL	2018	=	99	1983	=	10
MAY	2018	=	67	1983	=	9
JUNE	2020	=	99	1993	=	13
JULY	2012	=	89	1982	=	11
AUGUST	2018	=	71	1978	=	14
SEPTEMBER	2017	=	81	1977	=	8
OCTOBER	2010	=	67	1985	=	6
NOVEMBER	2020	=	85	1985	=	6
DECEMBER	2013	=	156	1982	=	9
	TOTAL		1031	TOTAL		117

YEAR		TOTAL RUNS	YEAR		TOTAL RUNS	YEAR		TOTAL RUNS
1986	=	204	1998	=	389	2010	=	620
1987	=	292	1999	=	446	2011	=	631
1988	=	313	2000	=	403	2012	=	536
1989	=	273	2001	=	397	2013	=	687
1990	=	253	2002	=	373	2014	=	566
1991	=	239	2003	=	485	2015	=	595
1992	=	240	2004	=	541	2016	=	613
1993	=	262	2005	=	550	2017	=	755
1994	=	304	2006	=	507	2018	=	772
1995	=	316	2007	=	472	2019	=	733
1996	=	328	2008	=	644	2020	=	785
1997	=	349	2009	=	595	**2021**	=	**71**

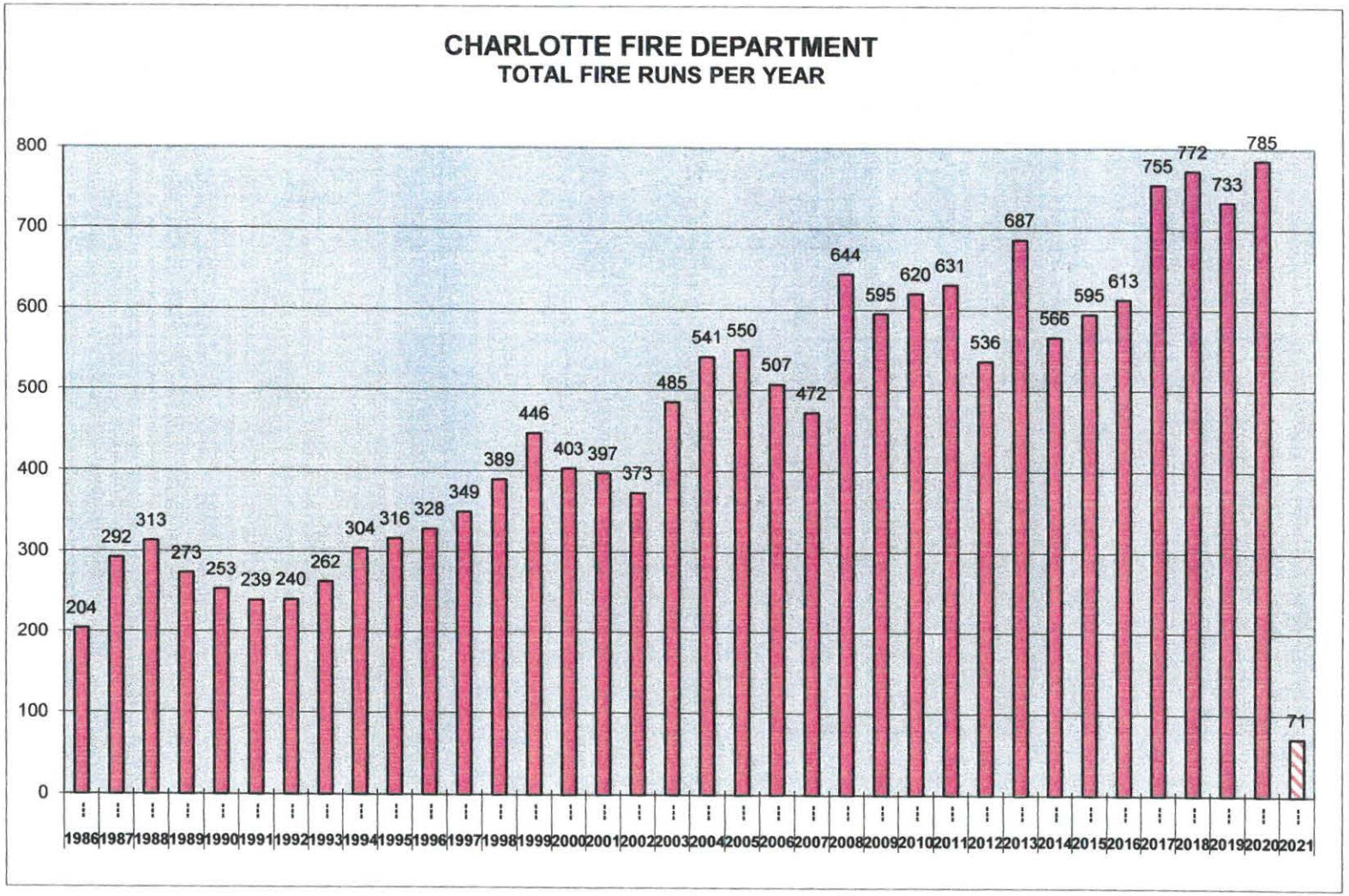
Total Fire Runs since Januay 1, 1976 = 17972

Average per year = 399

CHARLOTTE FIRE DEPARTMENT

FIRE RUN TOTALS -- JANUARY 1986 THROUGH JANUARY 2021

YEAR		TOTAL RUNS
1986	---	204
1987	---	292
1988	---	313
1989	---	273
1990	---	253
1991	---	239
1992	---	240
1993	---	262
1994	---	304
1995	---	316
1996	---	328
1997	---	349
1998	---	389
1999	---	446
2000	---	403
2001	---	397
2002	---	373
2003	---	485
2004	---	541
2005	---	550
2006	---	507
2007	---	472
2008	---	644
2009	---	595
2010	---	620
2011	---	631
2012	---	536
2013	---	687
2014	---	566
2015	---	595
2016	---	613
2017	---	755
2018	---	772
2019	---	733
2020	---	785
2021	---	71



THE CITY OF
CHARLOTTE
MICHIGAN

Erin LaPere <elapere@charlottemi.org>

Re cyber attack on Florida water plant

4 messages

Perry Thompson <perry@4coc.com> Fri, Feb 12, 2021 at 12:40 PM
To: Erin LaPere <elapere@charlottemi.org>
Cc: Ron Kramer <rkramer@charlottemi.org>, Amy Gilson <AGilson@charlottemi.org>

Ms. LaPere,

You recently asked about the security of our water treatment plant in light of the cyber-attack on a water facility in Florida. I have attached a pdf report from the US Cybersecurity & Infrastructure Security Agency. As part of our ongoing efforts to secure the City of Charlotte from cyber attacks, we regularly follow reports such as this without bothering you with details about all of them. But because of your inquiry I am attaching the report about this particular incident for your reference.

The short answer is that we are not susceptible to this attack. As the report indicates, remote access software was used to access a computer with outdated security and the ability to physically control the municipality's water treatment system.

Computer resources used to control physical plant are referred to as Operational Technology (OT) as opposed to the much more commonly discussed Information Technology (IT). Manipulating OT can cause direct physical harm either by making machines run out of control to damage themselves or by making them operate in an unintended way to cause other harm, such as changing the lye levels in the water supply.

Consistent with cybersecurity best practices, the OT network at our water treatment plant is separated from the IT portion of the network. Additionally, the OT network is not accessible from and does not communicate in any way with the IT network or the public Internet. We maintain a separate wireless network at WWTP so that while on premises WWTP personnel can remotely monitor and control devices in different buildings. For example, WWTP personnel frequently need to turn on a pump located in one building while monitoring an event in another building or in the outside tanks. Before this wireless network two people would be required to do the job or the results would be left unmonitored while the pump was activated.

To ensure security of the physical operations, this network is inaccessible outside the physical WWTP plant. The only link it has to the outside world is software that allows the control computer to place a phone call over the public switched telephone network in the event of an after hours alarm condition. These calls are made to specific numbers on a phone tree and use "plain old telephone service" (POTS), so they are not available as an attack vector for potential hackers.

The network I just described is at WWTP and thus these comments do not specifically address the city water supply. The security of the water supply "network" is even more clear. The one computer involved in management and monitoring of that system is located in a building that does not even have an internet connection or phone line. It is not connected in any way to the outside world. Thus the network is just the one computer and the machines it controls.

I will also point out that the attached report does mention some other things that will sound familiar from our IT network. For example, they mention that TeamViewer or similar remote access software seems to have been used to gain access to the machine and that the attacked machine appears to have been a Windows 7 machine with security vulnerabilities. While we do use several remote access products on the city's IT network for various reasons, these products are kept as secure as they can possibly be kept. For example, accounts that could be used to access or manage large portions of the network are protected by several two factor authentication mechanisms. Additionally, users in general have the least amount of authority needed to let them do their job. Thus if a hacker gained access to a particular account, they would not necessarily have access to the entire network. Finally, all servers and workstations on the city's network are protected by two of the best security products in the industry. I would prefer not to identify the specific products in a memo that I expect will become part of your report to the City Council, and thus readily available to the public. Revealing the exact security software used gives hackers an advantage when they are looking for weaknesses in your system.

Please let me know if you have any further questions, whether about this incident or cybersecurity in general.

Perry Thompson